

1 SPENCER PERSSON (State Bar No. 235054)  
spencerpersson@dwt.com  
2 COURTNEY DETHOMAS (State Bar No. 294591)  
courtneydethomas@dwt.com  
3 MONDER KHOURY (State Bar No. 312949)  
mikekhoury@dwt.com  
4 DAVIS WRIGHT TREMAINE LLP  
865 South Figueroa Street, 24th Floor  
5 Los Angeles, California 90017-2566  
Telephone: (213) 633-6800  
6 Fax: (213) 633-6899

7 Attorneys for Defendant  
TRINITY HEALTH CORPORATION  
8  
9

10 UNITED STATES DISTRICT COURT  
11 EASTERN DISTRICT OF CALIFORNIA  
12

13 JANE DOE, individually and on behalf  
of all others similarly situated,

14 Plaintiff,  
15

16 vs.

17 TRINITY HEALTH CORPORATION;  
and DOE DEFENDANTS 1-100;

18 Defendants.  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Case No. 1:21-at-00677

**NOTICE OF REMOVAL**

**DEMAND FOR JURY TRIAL**

[From the Superior Court of California,  
County of Fresno, Case No.  
21CECG01454]

Complaint Filed: May 20, 2021

Action Removed: June 23, 2021

1       **PLEASE TAKE NOTICE** that Defendant Trinity Health Corporation  
2 (“Trinity Health”) hereby removes this action from the Superior Court of the State  
3 of California for the County of Fresno to the United States District Court for the  
4 Eastern District of California, Fresno Division. Trinity Health is entitled to remove  
5 this action to federal district court pursuant to 28 U.S.C. §§ 1332(d), 1441 and 1453  
6 based on the following:

7           1.       On May 20, 2021, Plaintiff Jane Doe (Plaintiff), purportedly acting on  
8 her own behalf and on behalf of all others similarly situated, commenced an action  
9 in the Superior Court of the State of California in and for the County of Fresno,  
10 captioned *Doe v. Trinity Health Corporation, et. al*, Case No. 21CECG01454 (the  
11 State Court Action). A true and complete copy of the complaint in the State Court  
12 Action served upon Trinity Health is attached hereto as **Exhibit A** (the Complaint).

13           2.       Plaintiff asserts various causes of action related to the alleged  
14 unauthorized access, viewing, exfiltration, theft and disclosure of unencrypted  
15 medical and personal identifying information as a result of a security breach of  
16 third-party Accellion, Inc.’s File Transfer Appliance, which was allegedly used by  
17 Trinity Health and many other companies to transfer large files electronically.

18           3.       On May 24, 2021, Trinity Health was served with a copy of the  
19 Complaint and a summons from the State Court Action. This Notice of Removal is  
20 timely because it has been filed within thirty (30) days of service of the Summons  
21 and Complaint upon Trinity Health. *See* 28 U.S.C. § 1446(b); Fed. R. Civ. P.  
22 6(a)(1); *see also Murphy Bros., Inc. v. Michetti Pipe Stringing, Inc.*, 526 U.S. 344,  
23 354 (1999) (“[I]f the complaint is filed in court prior to any service, the removal  
24 period runs from the service of the summons.”).

25           4.       In addition to the Complaint, all other pleadings, processes, and orders  
26 served upon or received by Trinity Health in the State Court Action are attached  
27 hereto:

28           a.       The Summons is attached hereto as **Exhibit B**;

- b. The Civil Case Cover Sheet is attached hereto as **Exhibit C**;  
and
- c. The Notice of Case Management Conference and  
Assignment of Judge for All Purposes is attached hereto as  
**Exhibit D**.

### **The Action Is Removable**

5. The State Court Action is removable to this Court because the Court has original jurisdiction and the Eastern District of California encompasses the location in which the State Court Action is currently pending (*i.e.*, Fresno, California). *See* 28 U.S.C. § 1441(a) (“[A]ny civil action brought in a State court of which the district courts of the United States have original jurisdiction, may be removed by the defendant . . . to the district court of the United States for the district and division embracing the place where such an action is pending.”).

6. This Court has original jurisdiction pursuant to the Class Action Fairness Act of 2005 (CAFA). CAFA was enacted based on Congress’s concern that “cases involving large sums of money, citizens of many different States, and issues of national concern, have been restricted to State courts even though they have national consequences.” 151 Cong. Rec. S1086-02 (Feb. 8, 2005). CAFA’s purpose is to allow “federal court consideration of interstate cases of national importance under diversity jurisdiction.” *Luther v. Countrywide Home Loans Servicing LP*, 533 F.3d 1031, 1034 (9th Cir. 2008) (citing Pub. L. No. 109-2 § 2(b)(2)).

7. “[N]o antiremoval presumption attends cases invoking CAFA, which Congress enacted to facilitate adjudication of certain class actions in federal court.” *Dart Cherokee Basin Operating Co., LLC v. Owens*, 574 U.S. 82, 89 (2014). CAFA extends federal jurisdiction over class actions where: (1) any member of the proposed class is a citizen of a state different from any defendant (*i.e.*, minimal diversity exists); (2) there are at least 100 members in all proposed plaintiff classes

combined; and (3) the amount in controversy exceeds \$5 million. *See* 28 U.S.C. § 1332(d). As explained below, each of these requirements is satisfied in this case and no CAFA exceptions apply.

### **The Minimal Diversity Requirement Is Satisfied**

8. A class action is removable based on diversity jurisdiction if “any member of a class of plaintiffs is a citizen of a State different from any defendant.” 28 U.S.C. § 1332(d)(2)(A).

9. Contrary to the allegations in the Complaint, Defendant Trinity Health is not a citizen of California.<sup>1</sup> For diversity purposes under CAFA, a corporation is a citizen of the state of its incorporation and the state where its principal place of business is located. *See* U.S.C. § 1332(c). When the Complaint was filed and at the time of removal, Trinity Health was and remains incorporated under the laws of Indiana, with its principal place of business in Livonia, Michigan. *See Exhibit E*. Thus, for purposes of determining diversity jurisdiction, Trinity Health is a citizen of Indiana and/or Michigan. *See* 28 U.S.C. § 1332(c)(1); *see also Exhibit E*.

10. Plaintiff is a California resident and citizen. *See* Complaint ¶ 8. As such, at least one Plaintiff is not a citizen of Indiana or Michigan, satisfying minimal diversity. Trinity Health is unable to determine the citizenship of all of the class members, Plaintiff alleges no facts to suggest that they are citizens of Indiana or Michigan, nor would this impact minimal diversity. Ultimately,

---

<sup>1</sup> This Court may properly take judicial notice of **Exhibit E**, which is a certified document of public record, retrieved from the Indiana Secretary of State’s office at: <https://bsd.sos.in.gov/publicbusinesssearch>. Fed. R. Evid. 201; *United States v. Black*, 482 F.3d 1035, 1041 (9th Cir. 2007) (public records are proper subjects of judicial notice); *see also Lee v. City of Los Angeles*, 250 F.3d 668, 689 (9th Cir. 2001) (a court may take judicial notice of “matters of public record”); *Gaboratory, Inc. v. Gaboratory Int’l, Inc.*, No. CV 07-04725 MMM (EX), 2008 WL 11406072, at \*7 n.29 (C.D. Cal. Nov. 10, 2008) (taking judicial notice of secretary of state records and collecting cases doing the same).

1 Plaintiff has only alleged California causes of action that could not apply to citizens  
2 of Indiana or Michigan.

3 11. Citizenship of the remaining Doe Defendants in the action is irrelevant  
4 as removal is appropriate under CAFA without regard as to whether any other  
5 defendant is a local citizen. *See* 28 U.S.C. § 1453(b); 28 U.S.C. § 1332(d)(2)(A).

6 12. Therefore, there is sufficient diversity of citizenship between the  
7 parties in this case to permit removal.

8 **Plaintiff's Proposed Class Exceeds 100 Members**

9 13. For a class action to be removable under CAFA, “the number of  
10 members of all proposed plaintiff classes in the aggregate” must be at least 100. 28  
11 U.S.C. § 1332(d)(5)(B).

12 14. Plaintiff's proposed class exceeds 100 members. Plaintiff alleges in  
13 the Complaint that

14 California law requires a business to notify any California resident whose  
15 unencrypted personal information, as defined, was acquired, or reasonably  
16 believed to have been acquired, by an unauthorized person. California law  
17 also requires that a sample copy of a breach notice sent to more than 500  
18 California residents must be provided to the California Attorney General. On  
19 or about April 6, 2021, TRINITY HEALTH caused a form letter sent on its  
20 behalf, addressed to “Re: Patient,” signed by Monica Lareau in her capacity  
21 as “Privacy Official” of TRINITY HEALTH an exemplar . . . to be  
22 submitted to the Attorney General of the State of California and to be mailed  
23 to Plaintiff and the Class . . .

24 Complaint, ¶ 48.

25 15. Plaintiff also alleges that the security incident from which this case  
26 arises affected 586,869 persons. Complaint, ¶¶ 51, 54.

**The Amount in Controversy Exceeds \$5 Million**

16. To establish jurisdiction under CAFA, the amount in controversy must exceed \$5,000,000. *See* 28 U.S.C. § 1332(d).

17. The Complaint does not explicitly allege the amount-in-controversy, but this removal petition does so. Where, as here, “the plaintiff’s complaint does not state the amount in controversy, the defendant’s notice of removal may do so.” *Dart Cherokee Basin Operating Co., LLC v. Owens*, 574 U.S. 81, 84 (2014). To establish the amount in controversy, a notice of removal “need not contain evidentiary submissions.” *Id.* Rather, “a defendant’s notice of removal need include only a plausible allegation that the amount in controversy exceeds the jurisdictional threshold.” *Id.* at 89.

18. This action satisfies CAFA because the “potential damages could exceed the jurisdictional amount.” *Lewis v. Verizon Commc’ns, Inc.*, 627 F.3d 395, 397 (9th Cir. 2010) (noting removing defendant need only show “that the potential damages could exceed the jurisdictional amount”); *Woods v. CVS Pharm., Inc.*, No. 14-0259, 2014 U.S. Dist. LEXIS 13339, at \*5 (C.D. Cal. Jan. 30, 2014) (“The ultimate inquiry is what amount is put ‘in controversy’ by the plaintiff’s complaint, not what a defendant will actually owe.”) (citation omitted).

19. For purposes of removal only, and without conceding that Plaintiff or the class members are entitled to any damages, remedies, or penalties whatsoever in connection with their claims, the aggregated claims of the class establish that the amount in controversy exceeds the jurisdictional minimum of \$5,000,000, exclusive of interest and costs. *See* 28 U.S.C. § 1332(d)(2). The amount in controversy in this action easily satisfies CAFA’s \$5,000,000 jurisdictional threshold based on Plaintiff’s request for, among other things, (a) actual damages, (b) restitution, (c) attorneys’ fees, (d) injunctive relief and (e) statutory damages.

***Statutory Damages***

20. Potential statutory damages exceed the jurisdictional minimum.

21. In a class action, “the claims of the individual class members shall be aggregated to determine whether the matter in controversy exceeds the [jurisdiction minimum].” 28 U.S.C. § 1332(d)(6).

22. Here, the potential statutory damages alone may aggregate to exceed \$5 million. Plaintiff asserts a cause of action under California Civil Code §§ 56, *et seq* (Violations of the Confidentiality of Medical Information Act). Under California Civil Code § 56.36(b)(1), each individual harmed by a violation may be awarded “nominal damages of one thousand dollars.” Plaintiff’s Complaint is seeking \$1,000 per violation to Plaintiff individually and to each member of the Class. Complaint, at 35:16-18. The class need only include 5,000 persons to meet this threshold, and Plaintiff has alleged a class of 586,869 persons. Complaint, ¶¶ 51, 54.

23. For these reasons, the statutory damages amounts potentially at issue in this case bring the amount in controversy well over \$5 million.

### *Actual Damages*

24. Potential actual damages sought also satisfy the jurisdictional minimum.

25. While Trinity Health disputes Plaintiff's entitlement to any remedy or damages in any amount, these additional amounts sought, in conjunction with the other purported statutory damages above, push Plaintiff's claims further above the \$5,000,000 minimum jurisdictional threshold.

### *Attorneys' Fees*

26. The Plaintiff's potential attorneys' fees claim would supplement any other damages to compel this action to exceed the jurisdictional minimum.

27. Plaintiff seeks attorneys’ fees and costs as permitted by law pursuant to Code of Civil Procedure Civil Code § 1021.5, and under the “common fund” and “substantial benefit” doctrines, which Plaintiff alleges entitles her to an array of attorneys’ fees. Complaint, at 36:10-12.



28. Attorneys in class actions brought under California’s unfair competition and consumer protection statutes have sought attorneys’ fees in the millions of dollars. *See, e.g., Brown v. Hain Celestial Group, Inc.*, No. 11-3082, 2016 U.S. Dist. LEXIS 20118 (N.D. Cal. Feb. 18, 2016) (UCL, FAL, and CLRA mislabeling class action; seeking approval in excess of \$3 million in fees); *Hendricks v. StarKist Co.*, No.13-729, 2016 U.S. Dist. LEXIS 134872 (N.D. Cal. Sept. 29, 2016) (same); *Retta v. Millennium Products, Inc.*, No. 15–1801, 2017 U.S. Dist. LEXIS 220288 (C.D. Cal. Aug. 22, 2017) (same; seeking approval in excess of \$2 million).

29. These amounts may also be included in the amount in controversy for purposes of removal. *See Galt G/S v. JSS Scandinavia*, 142 F.3d 1150, 1155-56 (9th Cir. 1998); *Brady v. Mercedes-Benz USA, Inc.*, 243 F. Supp. 2d 1004, 1010-11 (N.D. Cal. 2002) (using “amount of fees commonly incurred in similar litigation” as reasonable measure of attorney’s fees to determine amount in controversy).

### ***Injunctive Relief***

30. The cost to Trinity Health to comply with injunctive relief sought by Plaintiff also shows that the amount in controversy for this matter potentially exceeds the jurisdictional minimum. Complaint, at 35:26, Prayer for Relief.

31. The “value” of the injunctive relief for purposes of the jurisdictional inquiry depends on the value to the plaintiff or the cost to the defendant if such relief is granted. *See Corral v. Select Portfolio Servicing, Inc.*, 878 F.3d 770, 775 (9th Cir. 2017); *In re Ford Motor Co./Citibank (S.D.), N.A.*, 264 F.3d 952, 958 (9th Cir. 2001) (“where the value of a plaintiff’s potential recovery (in this case, a maximum of \$3,500) is below the jurisdictional amount, but the potential cost to the defendant of complying with the injunction exceeds that amount, it is the latter that represents the amount in controversy for jurisdictional purposes”). Here, Plaintiff seeks to enjoin Trinity Health from the conduct she considers in violation of Civil Code § 1798. Although Trinity Health disputes that Plaintiff is entitled to



1 any such remedy, the value of any injunctive relief awarded to Plaintiff—measured  
2 by the cost to Trinity Health—serves to put Plaintiff’s claims further above the  
3 \$5,000,000 threshold.

4 32. In sum, based on Plaintiff’s assertions and theories of recovery, the  
5 amount in controversy well exceeds \$5,000,000.

6 **No CAFA Exception Applies.**

7 33. CAFA “confers subject matter jurisdiction and provides express  
8 ‘exceptions’ to the exercise of that jurisdiction.” *Serrano v. 180 Connect, Inc.*, 478  
9 F.3d 1018, 1024 (9th Cir. 2007). Although “the removing party bears the initial  
10 burden of establishing federal jurisdiction under § 1332(d)(2), once federal  
11 jurisdiction has been established under that provision, the objecting party bears the  
12 burden of proof as to the applicability of any express statutory exception under  
13 §§ 1332(d)(4) (A) and (B).” *Id.*

14 34. Plaintiff has not met her burden in establishing that any CAFA  
15 exceptions apply here.

16 35. Plaintiff does not allege a mass action.

17 36. Plaintiff does not allege a securities action.

18 37. Plaintiff does not allege a corporate governance claim.

19 38. “[T]he ‘home state’ and ‘local controversy’ exceptions to the CAFA  
20 apply only if ‘the primary defendants are citizens of the State in which the action  
21 was originally filed,’ 28 U.S.C. § 1332(d)(3), or if at least one defendant ‘is a  
22 citizen of the State in which the action was originally filed,’ 28 U.S.C. §  
23 1332(d)(4).” *Korn v. Polo Ralph Lauren Corp.*, 536 F. Supp. 2d 1199, 1206 (E.D.  
24 Cal. 2008). Trinity Health is the only named defendant in this action. As  
25 demonstrated above, Trinity Health is a citizen of Indiana and Michigan for  
26 purposes of diversity jurisdiction.  
27  
28

**Trinity Health Satisfies the Requirements of 28 U.S.C. § 1446**

39. This Notice of Removal is signed pursuant to Rule 11 of the Federal Rules of Civil Procedure. *See* 28 U.S.C. § 1446(a).

40. This Notice of Removal has been filed within thirty days of service of the Complaint and summons on Trinity Health.

41. Concurrently with the filing of this Notice, Trinity Health will give written notice to all adverse parties and will file a copy of this Notice with the clerk of the Superior Court of the State of California in and for the County of Fresno. *See* 28 U.S.C. § 1446(d).

42. There are no other defendants from which Trinity Health may obtain consent prior to removal; nor is Trinity Health required to obtain the consent of any other defendants to this action prior to seeking removal. *See* 28 U.S.C. § 1453(b).

43. Trinity Health does not waive, and expressly preserves, all objections, defenses, and exceptions authorized by law, including but not limited to those permitted pursuant to Rules 4 and 12 of the Federal Rules of Civil Procedure.

DATED: June 23, 2021

DAVIS WRIGHT TREMAINE LLP  
SPENCER PERSSON  
COURTNEY DETHOMAS  
MONDER KHOURY

By: /s/Spencer Persson

Attorneys for Defendant  
TRINITY HEALTH CORPORATION

**DEMAND FOR JURY TRIAL**

Defendant Trinity Health hereby preserves its right to a jury and for that reason demands a jury at this time for any issues so triable.

DATED: June 23, 2021

DAVIS WRIGHT TREMAINE LLP  
SPENCER PERSSON  
COURTNEY DETHOMAS  
MONDER KHOURY

By: /s/Spencer Persson

Attorneys for Defendant  
TRINITY HEALTH CORPORATION

# EXHIBIT A

Patrick N. Keegan, Esq. (SBN 167698)  
pkeegan@keeganbaker.com  
**KEEGAN & BAKER, LLP**  
2292 Faraday Avenue, Suite 100  
Carlsbad, CA 92008  
Telephone: (760) 929-9303  
Facsimile: (760) 929-9260

E-FILED  
5/20/2021 7:23 PM  
Superior Court of California  
County of Fresno  
By: A. Rodriguez, Deputy

Attorneys for Plaintiff JANE DOE

**SUPERIOR COURT OF THE STATE OF CALIFORNIA  
FOR THE COUNTY OF FRESNO**

JANE DOE, individually and on behalf of all  
others similarly situated,

Plaintiff,

vs.

TRINITY HEALTH CORPORATION; and DOE  
DEFENDANTS 1-100;

Defendants.

Case No.: 21CECG01454

**CLASS ACTION COMPLAINT FOR  
DAMAGES, RESTITUTION, AND  
INJUNCTIVE RELIEF FOR VIOLATIONS  
OF:**

- (1) **THE CONFIDENTIALITY OF  
MEDICAL INFORMATION ACT,  
CIVIL CODE §§ 56, *ET SEQ.*;**
- (2) **BREACH OF CALIFORNIA  
SECURITY NOTIFICATION  
LAWS, CALIFORNIA CIVIL CODE  
§ 1798.82; AND**
- (3) **BUSINESS AND PROFESSIONS  
CODE §§ 17200, *ET SEQ.***

**JURY TRIAL DEMANDED**

Plaintiff JANE DOE (or "Plaintiff"), by and through her attorneys, bring this class action on behalf of herself individually and all others similarly situated, against Defendants TRINITY HEALTH CORPORATION and DOE DEFENDANTS 1-100 (collectively referred to as "Defendants"), and alleges upon information and belief as follows:

**INTRODUCTION**

1. This class action arises from the negligent and failure of Defendants to properly create, maintain, preserve, and/or store confidential, medical and personal identifying information of Plaintiff<sup>1</sup> and all other persons similarly situated which allowed an unauthorized person to gain

<sup>1</sup> California statutory law specifically allows a party to bring a lawsuit using a pseudonym in cases involving health care patients. Cal. Civ. Code § 3427.3 (West 2011). Specifically, section 3427.3

1 access to an email file transfer platform of Defendants prior to and in May of 2020, causing  
 2 unauthorized access, viewing, exfiltration, theft, and disclosure of unencrypted medical and  
 3 personal identifying information of Plaintiff and other persons similarly situated, to at least one  
 4 unauthorized person resulting in violations of the Confidentiality of Medical Information Act, Civil  
 5 Code §§ 56, *et seq.* (hereinafter referred to as the “Act”), the Security Notification Laws, Civil Code  
 6 § 1798.82, and the Business and Professions Code §§ 17200 *et seq.* Under the Act, Plaintiff, and  
 7 all other persons similarly situated, have the right to expect that the confidentiality of their medical  
 8 information in possession of Defendants and/or derived from Defendants to be reasonably  
 9 preserved and protected from unauthorized access, viewing, exfiltration, theft, and disclosure.

10 2. As alleged more fully below, failing to take adequate and reasonable measures to  
 11 ensure its data systems were protected against unauthorized intrusions, by failing to invest in cyber  
 12 security and data protection safeguards, failing to implement adequate and reasonable security  
 13 controls and user authorization and authentication processes, failing to limit the types of data  
 14 permitted to be transferred, failing to properly and adequately educate and train its employees, and  
 15 to put into place reasonable or adequate computer systems and security practices to safeguard  
 16 customers’ and patients’ medical and personal identifying information, Defendants negligently  
 17 created, maintained, preserved, and stored Plaintiff’s and the Class (defined *infra*) members’  
 18 medical and personal identifying information in possession of or derived from Defendants allowed  
 19 such information to be accessed, downloaded, stolen and viewed by at least one unauthorized third  
 20 party user, without Plaintiff’s and the Class members’ prior written authorization, which constitutes  
 21 unauthorized disclosure and/or release of their information in violation of Civil Code §§ 56.10(a)  
 22 and 56.101(a) of the Act. In fact, Defendant TRINITY HEALTH CORPORATION’s form letter,  
 23

24  
 25 provides, “The court having jurisdiction over a civil proceeding under this title shall take all steps  
 26 ***reasonably necessary to safeguard the individual privacy and prevent harassment of a health care***  
 27 ***patient***, licensed health practitioner, or employee, client, or customer of a health care facility who is  
 28 a party or witness in the proceeding, including granting protective orders. ***Health care patients***,  
 licensed health practitioners, and employees, clients, and customers of the health care facility ***may***  
***use pseudonyms to protect their privacy.***” Cal. Civ. Code § 3427.3 (emphasis added). Here, a  
 pseudonym has been used in place of the real name of Plaintiff because at all times relevant to this  
 action, Plaintiff is a health care patient under Civil Code § 56.05(k) and has individual privacy  
 concerns and a reasonable fear of harassment in light of the nature of the case.

1 addressed to “Re: Patient,” signed by Monica Lareau in her capacity as “Privacy Official,” sent to  
 2 Plaintiff and all other persons similarly situated, stating in part, “because the patient listed above  
 3 receives service from a hospital or health care provider that is a current or former member of Trinity  
 4 Health,” and informing her, in part, of “an incident that may impact the privacy of certain  
 5 confidential information related to the patient. Trinity Health was recently notified by Accellion, a  
 6 third-party vendor, of a security incident. The Accellion File Transfer Appliance is used by Trinity  
 7 Health and many other companies for large file transfer service.... **What Happened?** On January  
 8 29, 2021, Accellion informed Trinity Health of a security issue with its secure file transfer platform,  
 9 used for sending secure email. Upon receiving this notice, Trinity Health ... launched an  
 10 investigation into the issue and its impact on both Trinity Health and our patients and colleagues.  
 11 This investigation determined that certain files present on the appliance on January 20 were  
 12 downloaded by an unknown user.... **What Information is Involved?** Although the investigation is  
 13 ongoing, on February 4, 2021, we determined file(s) were present on the appliance at the time of  
 14 this event. The files contained certain protected health information, including some combination of  
 15 the **following patient’s name, address, email, date of birth, healthcare provider, dates and**  
 16 **types of healthcare services, medical record number, immunization type, lab results,**  
 17 **medications, payment, payer name and claims information.”** An exemplar of Defendant  
 18 TRINITY HEALTH CORPORATION’s form letter, addressed to “Re: Patient,” signed by Monica  
 19 Lareau in her capacity as “Privacy Official,” submitted to the Attorney General of the State of  
 20 California is attached hereto as **Exhibit A**.

21 3. Because the individually identifiable medical information and other personal  
 22 identifying information of Plaintiff and the Class was subject to unauthorized access, download and  
 23 viewing by at least one unauthorized third party “user” and in violation of the Act, Plaintiff,  
 24 individually and on behalf of all others similarly situated, seeks from Defendants nominal damages  
 25 in the amount of one thousand dollars (\$1,000) for each violation under Civil Code §56.36(b)(1)  
 26 and actual damages, according to proof, for each violation pursuant to Civil Code § 56.36(b)(2).  
 27 Further, because Plaintiff also alleges Defendants’ conduct violates Business & Professions Code  
 28



1 §§ 17200, *et seq.*, Plaintiff, individually and on behalf of others similarly situated, seeks injunctive  
2 relief and restitution from Defendants under Business and Professions Code § 17203.

3 4. This action, if successful, will enforce an important right affecting the public interest  
4 and would confer a significant benefit, whether pecuniary or non-pecuniary, on a large class of  
5 persons. Private enforcement is necessary and places a disproportionate financial burden on Plaintiff  
6 in relation to Plaintiff's stake in the matter, and therefore class certification is appropriate in this  
7 matter.

8 **JURISDICTION AND VENUE**

9 5. This Court has jurisdiction over this action under California Code of Civil Procedure  
10 § 410.10. The aggregated amount of damages incurred by Plaintiff and the Class in the aggregate  
11 exceeds the \$25,000 jurisdictional minimum of this Court. Further, the amount in controversy as to  
12 Plaintiff individually does not exceed \$75,000.

13 6. Venue is proper in this Court under California Bus. & Prof. Code § 17203, Code of  
14 Civil Procedure §§ 395(a) and 395.5 because Defendant TRINITY HEALTH CORPORATION is  
15 registered to do business in and does business in the State of California, and employs persons  
16 located in the County of Fresno and in this judicial district. Defendants have obtained medical  
17 information of Plaintiff and the Class in the transaction of business in the State of California and in  
18 this judicial district, which has caused both obligations and liability of Defendants to arise in the  
19 State of California and in this judicial district.

20 7. Further, this action does not qualify for federal jurisdiction under the Class Action  
21 Fairness Act because the home-state controversy exception under 28 U.S.C. § 1332(d)(4)(B) applies  
22 to this action because (1) more than two-thirds of the members of the proposed Class are citizens of  
23 the State of California, and (2) Defendants are both citizens of the State of California.

24 **PARTIES**

25 **A. PLAINTIFF**

26 8. Plaintiff JANE DOE is and was at all times relevant to this action a resident of the  
27 State of California and citizen of the State of California. At all times relevant to this action,  
28 Plaintiff JANE DOE was a patient of, received medical treatment and diagnosis from, and provided

1 her personal information, including her name, address, date of birth, social security number, phone  
2 number and email address to Defendant TRINITY HEALTH CORPORATION. Additionally,  
3 Plaintiff received a letter at her residential address, sent on TRINITY HEALTH CORPORATION's  
4 behalf, addressed in her name as "Re: Patient," dated April 6, 2021, signed by Monica Lareau in her  
5 capacity as "Privacy Official," stating in part, "because the patient listed above receives service  
6 from a hospital or health care provider that is a current or former member of Trinity Health," and  
7 informing her, in part, of "an incident that may impact the privacy of certain confidential  
8 information related to the patient. Trinity Health was recently notified by Accellion, a third-party  
9 vendor, of a security incident. The Accellion File Transfer Appliance is used by Trinity Health and  
10 many other companies for large file transfer service.... **What Happened?** On January 29, 2021,  
11 Accellion informed Trinity Health of a security issue with its secure file transfer platform, used for  
12 sending secure email. Upon receiving this notice, Trinity Health ... launched an investigation into  
13 the issue and its impact on both Trinity Health and our patients and colleagues. This investigation  
14 determined that certain files present on the appliance on January 20 were downloaded by an  
15 unknown user.... **What Information is Involved?** Although the investigation is ongoing, on  
16 February 4, 2021, we determined file(s) were present on the appliance at the time of this event. The  
17 files contained certain protected health information, including some combination of the **following**  
18 **patient's name, address, email, date of birth, healthcare provider, dates and types of**  
19 **healthcare services, medical record number, immunization type, lab results, medications,**  
20 **payment, payer name and claims information."** As a result, Plaintiff reasonably fears that  
21 disclosure and/or release of her medical information created, maintained, preserved and/or stored on  
22 Defendants' email and computer network could subject her to harassment or abuse.

23 **B. DEFENDANTS**

24 9. Defendant TRINITY HEALTH CORPORATION ("TRINITY HEALTH") is  
25 registered to do business and does business in the State of California (Entity File No. C1866107),  
26 operates a principal place of business and a hospital identified as Saint Agnes Medical Center  
27 located at 1303 East Herndon Avenue, Fresno, CA 93720, and with its registered agent of service of  
28 process CT Corporation System located at 818 West Seventh Street, Suite 930, Los Angeles, CA

1 90017. At all times relevant to this action, TRINITY HEALTH was and is a provider of health care  
 2 who created, maintained, preserved, and stored personal and confidential medical information, as  
 3 that term is defined and set forth in the Act, including patient's name, address, email, date of birth,  
 4 healthcare provider, dates and types of healthcare services, medical record number, immunization  
 5 type, lab results, medications, payment, payer name and claims information, of Plaintiff and the  
 6 Class (defined *infra*), and is subject to the requirements and mandates of the Act, including but not  
 7 limited to Civil Code §§ 56.10, 56.101 and 56.36. On its website, TRINITY HEALTH represents  
 8 that it is a "health system serving communities across the country with 92 hospitals and thousands  
 9 of physicians and primary, specialty, and continuing care centers in 22 states," and TRINITY  
 10 HEALTH represents that "Saint Agnes Medical Center" located at "1303 E Herndon Ave  
 11 Fresno, CA 93720" is one of "Our locations."<sup>2</sup> On its website, TRINITY HEALTH represents that  
 12 "Our online patient portals allow you to access your medical information 24 hours a day, seven days  
 13 a week. These secure websites allow you to privately view basic lab results, portions of your  
 14 medical record, hospital discharge instructions and more."<sup>3</sup>; and sets forth a link to "Saint Agnes  
 15 Medical Center, Fresno" hospital,<sup>4</sup> which states "Our online patient portal, **mySaintAgnes**, enables  
 16 patients to conveniently access portions of their hospital medical records and view test results.  
 17 mySaintAgnes is a free, easy and secure way for patients to view their electronic medical records,  
 18 all from the convenience and privacy of your own home — 24 hours a day, seven days a week!"<sup>5</sup>  
 19 On or about April 6, 2021, TRINITY HEALTH caused a form letter sent on its behalf, addressed to  
 20 "Re: Patient," signed by Monica Lareau in her capacity as "Privacy Official" of TRINITY  
 21 HEALTH, an exemplar of which is attached hereto as **Exhibit A**, to be submitted to the Attorney  
 22 General of the State of California and to be mailed to Plaintiff and all others similarly situated.  
 23 Thus, at all times relevant to this action, TRINITY HEALTH was and is a "provider" of health  
 24 care and employed and employs persons located in the County of Fresno and in this judicial  
 25 district.

26 \_\_\_\_\_  
 27 <sup>2</sup> (<https://www.trinity-health.org/patient-portals/>, last visited May 19, 2021).

28 <sup>3</sup> (<https://www.trinity-health.org/find-a-location/>, last visited May 19, 2021).

<sup>4</sup> (<https://www.trinity-health.org/find-a-location/>, last visited May 19, 2021).

<sup>5</sup> (<https://www.samc.com/mysaintagnes/>, last visited May 19, 2021).

1           10. At all times relevant to this action, TRINITY HEALTH was and is a “business”  
2 within the meaning of Civil Code § 1798.140(c)(1), owns or licenses computerized data which  
3 includes Plaintiff’s and the Class’ personal information, within the meaning of Civil Code §  
4 1798.82(h), collected Plaintiff’s and the Class’ personal information within the meaning of Civil  
5 Code § 1798.81.5(d)(1)(A).

6           11. TRINITY HEALTH’s third-party vendor Accellion, Inc. (“ACCELLION”), a non-  
7 party, is registered to do business and does business in the State of California. Copies of  
8 ACCELLION’s Press Releases concerning this security incident are attached hereto as **Exhibit B**  
9 and **Exhibit C**.

10 **C. DOE DEFENDANTS**

11           12. The true names and capacities, whether individual, corporate, associate, or otherwise,  
12 of Defendants sued herein as DOE DEFENDANTS 1 through 100, inclusive, are currently unknown  
13 to Plaintiff, who therefore sues the Defendants by such fictitious names under the Code of Civil  
14 Procedure § 474. Each of the Defendants designated herein as a DOE DEFENDANT is legally  
15 responsible in some manner for the unlawful acts referred to herein. Plaintiff will seek leave of  
16 court and/or amend this complaint to reflect the true names and capacities of the Defendants  
17 designated hereinafter as DOE DEFENDANTS 1 through 100 when such identities become known.  
18 Any reference made to a named Defendant by specific name or otherwise, individually or plural, is  
19 also a reference to the actions or inactions of DOE DEFENDANTS 1 through 100, inclusive.

20 **D. AGENCY/AIDING AND ABETTING**

21           13. At all times herein mentioned, Defendants, and each of them, were an agent or joint  
22 venturer of each of the other Defendants, and in doing the acts alleged herein, were acting with the  
23 course and scope of such agency. Each Defendant had actual and/or constructive knowledge of the  
24 acts of each of the other Defendants, and ratified, approved, joined in, acquiesced and/or authorized  
25 the wrongful acts of each co-defendant, and/or retained the benefits of said wrongful acts.

26           14. Defendants, and each of them, aided and abetted, encouraged and rendered  
27 substantial assistance to the other Defendants in breaching their obligations to Plaintiff and the  
28 Class, as alleged herein. In taking action, as particularized herein, to aid and abet and substantially

1 assist the commissions of these wrongful acts and other wrongdoings complained of, each of the  
2 Defendants acted with an awareness of his/her/its primary wrongdoing and realized that his/her/its  
3 conduct would substantially assist the accomplishment of the wrongful conduct, wrongful goals,  
4 and wrongdoing.

5 **FACTUAL ALLEGATIONS**

6 15. At all times relevant to this action, including the period prior to and on January 20,  
7 2021, TRINITY HEALTH created, maintained, preserved, and stored records of the care, services  
8 and products, including the names, addresses, email addresses, dates of birth, healthcare providers,  
9 dates and types of healthcare services, medical record numbers, immunization types, lab results,  
10 medications, payments, payer names and claims information of Plaintiff and the Class (all of which  
11 constitutes medical information, as that term is defined and set forth in the Act), that Plaintiff and  
12 other Class members received in the State of California from TRINITY HEALTH and other  
13 TRINITY HEALTH providers of health care, on its email and computer network. As a result, at all  
14 times relevant to this action, including the period prior to and on January 20, 2021, TRINITY  
15 HEALTH was and is a “provider of health care” within the meaning of Civil Code § 56.05(m). As  
16 a result, at all times relevant to this action, including the period prior to and on January 20, 2021,  
17 Plaintiff and Class members were patients, within the meaning of Civil Code § 56.05(k), of  
18 TRINITY HEALTH and/or other TRINITY HEALTH providers of health care.

19 16. As a result, on or before January 20, 2021, Defendants possessed Plaintiff’s and the  
20 Class’ medical information, in electronic and physical form, in possession of or derived  
21 from Defendants regarding their medical history, mental or physical condition, or treatment. Such  
22 medical information included or contained an element of personal identifying information sufficient  
23 to allow identification of Plaintiff and the Class, such as their names, addresses, dates of birth,  
24 social security numbers, phone numbers and/or email addresses, or other information that, alone or  
25 in combination with other publicly available information, reveals their identity.

26 17. At all times relevant to this action, including the period prior to and on January 20,  
27 2021, pursuant to Civil Code § 56.06(a), TRINITY HEALTH, as a business that created,  
28 maintained, preserved, and stored records of the care, products and services that the Class members

1 received in the State of California from TRINITY HEALTH and/or other TRINITY HEALTH  
2 providers of health care, and/or other health care service plans, pharmaceutical companies, and  
3 contractors as defined by the Act, is and was, at all times relevant to this action, organized for the  
4 purpose of maintaining medical information, within the meaning of Civil Code § 56.05(j), in order  
5 to make the information available to an individual or to a provider of health care at the request of  
6 the individual or a provider of health care, for purposes of allowing the individual to manage his or  
7 her information, or for the diagnosis and treatment of the individual, is deemed to be a “provider of  
8 health care,” within the meaning of Civil Code § 56.05(m).

9 18. Alternatively, at all times relevant to this action, including prior to and on January  
10 20, 2021, pursuant to Civil Code § 56.05(d), TRINITY HEALTH, as an “entity that is a medical  
11 group, independent practice association, pharmaceutical benefits manager, or a medical service  
12 organization and is not a health care service plan or provider of health care,” is and was a  
13 “contractor” under Civil Code § 56.05(d).

14 19. Alternatively, at all times relevant to this action, including prior to and on January  
15 20, 2021, pursuant to Civil Code § 56.13, TRINITY HEALTH is and was a “recipient of medical  
16 information pursuant to an authorization as provided by this chapter or pursuant to the provisions of  
17 subdivision (c) of Section 56.10” and was prohibited from “further disclos[ing] that medical  
18 information except in accordance with a new authorization that meets the requirements of Section  
19 56.11, or as specifically required or permitted by other provisions of this chapter or by law.”

20 20. Alternatively, at all times relevant to this action, including prior to and on January  
21 20, 2021, pursuant to Civil Code § 56.245, TRINITY HEALTH is and was a “recipient of medical  
22 information pursuant to an authorization as provided by this chapter” and was prohibited from  
23 “further disclos[ing] such medical information unless in accordance with a new authorization that  
24 meets the requirements of Section 56.21, or as specifically required or permitted by other provisions  
25 of this chapter or by law.”

26 21. Additionally, at all times relevant to this action, including prior to and on January 20,  
27 2021, pursuant to Civil Code § 56.26(a), TRINITY HEALTH is and was an “entity engaged in the  
28 business of furnishing administrative services to programs that provide payment for health care



services” and was prohibited from “knowingly us[ing], disclos[ing] or permit[ing] its employees or agents to use or disclose medical information possessed in connection with performing administrative functions for a program, except as reasonably necessary in connection with the administration or maintenance of the program, or as required by law, or with an authorization.”

22. As a provider of health care, a contractor, and/or other authorized recipient of personal and confidential medical information, TRINITY HEALTH is required by the Act to ensure that medical information regarding patients is not disclosed or disseminated or released without patients’ authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

23. As provider of health care, a contractor, and/or other authorized recipient of personal and confidential medical information, TRINITY HEALTH is required by the Act not to disclose medical information regarding a patient without first obtaining an authorization<sup>6</sup> under Civil Code §§ 56.10, 56.13, 56.245 and 56.26.

---

<sup>6</sup> An “authorization” is defined under the Act as obtaining permission in accordance with Civil Code § 56.11. Under Civil Code § 56.11, an authorization for the release of medical information is valid only if it:

(a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type.

(b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization.

(c) Is signed and dated by one of the following:

(1) The patient. A patient who is a minor may only sign an authorization for the release of medical information obtained by a provider of health care, health care service plan, pharmaceutical company, or contractor in the course of furnishing services to which the minor could lawfully have consented under Part 1 (commencing with Section 25) or Part 2.7 (commencing with Section 60).

(2) The legal representative of the patient, if the patient is a minor or an incompetent. However, authorization may not be given under this subdivision for the disclosure of medical information obtained by the provider of health care, health care service plan, pharmaceutical company, or contractor in the course of furnishing services to which a minor patient could lawfully have consented under Part 1 (commencing with Section 25) or Part 2.7 (commencing with Section 60).

(3) The spouse of the patient or the person financially responsible for the patient, where the medical information is being sought for the sole purpose of processing an application for health insurance or for enrollment in a nonprofit hospital plan, a health care service plan, or an employee benefit plan, and where the patient is to be an enrolled spouse or dependent under the policy or plan.

(4) The beneficiary or personal representative of a deceased patient.

(d) States the specific uses and limitations on the types of medical information to be disclosed.

(e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information.

(f) States the name or functions of the persons or entities authorized to receive the medical information.

(g) States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information.

(h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information.

(i) Advises the person signing the authorization of the right to receive a copy of the authorization.



1       24. As a provider of health care, a contractor, and/or other authorized recipient of  
2 personal and confidential medical information, TRINITY HEALTH is required by the Act to create,  
3 maintain, preserve, and store medical records in a manner that preserves the confidentiality of the  
4 information contained therein under Civil Code § 56.101(a).

5       25. As provider of health care, a contractor, and/or other authorized recipient of personal  
6 and confidential medical information, TRINITY HEALTH is required by the Act to protect and  
7 preserve confidentiality of electronic medical information of Plaintiff and the Class in its possession  
8 under Civil Code § 56.101(b)(1)(A).

9       26. As a provider of health care, a contractor, and/or other recipient of medical  
10 information, TRINITY HEALTH is required by the Act to take appropriate preventive actions to  
11 protect the confidential information or records against release consistent with TRINITY HEALTH's  
12 obligations under the Act, under Civil Code § 56.36(e)(2)(E), or other applicable state law, and the  
13 Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) (HIPAA) and all  
14 HIPAA Administrative Simplification Regulations in effect on January 1, 2012, contained in Parts  
15 160, 162, and 164 of Title 45 of the Code of Federal Regulations, and Part 2 of Title 42 of the Code  
16 of Federal Regulations, including, but not limited to, all of the following:

- 17       i. Developing and implementing security policies and procedures.  
18       ii. Designating a security official who is responsible for developing and implementing  
19 its security policies and procedures, including educating and training the workforce.  
20       iii. Encrypting the information or records, and protecting against the release or use of  
21 the encryption key and passwords, or transmitting the information or records in a  
22 manner designed to provide equal or greater protections against improper  
23 disclosures.

24       27. At all times relevant to this action, including the period prior to and on January 20,  
25 2021, TRINITY HEALTH created, maintained, preserved, and stored Plaintiff's and the Class  
26 members' medical information on its Accellion File Transfer Appliance in an un-encrypted format.

27       28. At all times relevant to this action, including the period prior to and on January 20,  
28 2021, TRINITY HEALTH created, maintained, preserved, stored, disclosed and/or delivered

1 Plaintiff's and the Class members' medical information to ACCELLION on its Accellion File  
2 Transfer Appliance. At all times relevant to this action, TRINITY HEALTH did not obtain written  
3 authorization from the Plaintiff and the Class prior to creating, maintaining, preserving, storing,  
4 disclosing and/or delivering Plaintiff's and the Class members' medical information to  
5 ACCELLION on its Accellion File Transfer Appliance. Furthermore, TRINITY HEALTH's  
6 disclosure of and/or delivery of Plaintiff's and the Class members' medical information to  
7 ACCELLION on its Accellion File Transfer Appliance was not permissible without written  
8 authorization from the Plaintiff and the Class or under any exemption under Civil Code § 56.10(c).

9       29. By law, the HIPAA Privacy Rule applies only to covered entities, e.g. health care  
10 providers. However, most health care providers do not carry out all of their health care activities  
11 and functions by themselves. Instead, they often use the services of a variety of other persons or  
12 businesses. The Privacy Rule allows covered providers to disclose protected health information  
13 (PHI) to these "business associates" if the providers obtain assurances that the business associate  
14 will use the information only for the purposes for which it was engaged by the covered entity, will  
15 safeguard the information from misuse, and will help the covered entity comply with some of the  
16 covered entity's duties under the Privacy Rule. Covered entities may disclose PHI to an entity in its  
17 role as a business associate only to help the covered entity carry out its health care functions – not  
18 for the business associate's independent use or purposes, except as needed for the proper  
19 management and administration of the business associate. The Privacy Rule requires that a covered  
20 entity obtain assurances from its business associate that the business associate will appropriately  
21 safeguard the PHI it receives or creates on behalf of the covered entity. The satisfactory assurances  
22 must be in writing, whether in the form of a contract or other agreement between the covered entity  
23 and the business associate.

24       30. When hiring and monitoring a service provider or business associate such as  
25 ACCELLION, TRINITY HEALTH knew or should have known that it had a duty to inquire about  
26 potential service providers' and business associates' cybersecurity programs and how such  
27 programs are maintained. TRINITY HEALTH knew or should have known that it had a duty to  
28 compare potential service providers' and business associates' cybersecurity programs to the

1 industry standards adopted by other healthcare providers, and should evaluate potential service  
2 providers' track records in the industry by reviewing public information about data security  
3 incidents and litigation. TRINITY HEALTH knew or should have known that it had a duty to also  
4 ask potential service providers and business associates about whether they have experienced any  
5 cybersecurity incidents and how such incidents were handled, as well as whether the potential  
6 service provider has an insurance policy in place that would cover losses caused by cybersecurity  
7 breaches (including losses caused by internal and external threats). TRINITY HEALTH knew or  
8 should have known that it had a duty to review service provider and business associates contracts to  
9 ensure that the contracts require the service providers to comply, on an ongoing basis, with  
10 cybersecurity and information security standards (and avoid contract provisions that limit service  
11 providers' responsibility for cybersecurity and information technology breaches). Finally, TRINITY  
12 HEALTH knew or should have known that it had a duty to pay particular attention to contract terms  
13 relating to confidentiality, the use and sharing of information, notice by the vendor of cybersecurity  
14 risk assessments and audit reports, cybersecurity breaches and records retention and destruction.

15 31. Alternatively, Plaintiff alleges on information and belief that TRINITY HEALTH's  
16 disclosure of and/or delivery of Plaintiff's and the Class members' medical information to  
17 ACCELLION or use of its Accellion File Transfer Appliance was either without a business  
18 associate agreement or pursuant to a business associate agreement that was not permissible under  
19 the Privacy Rule or any exemption under Civil Code § 56.10(c), and/or because TRINITY  
20 HEALTH negligently failed to obtain reasonable assurances and negligently failed to monitor and  
21 conduct assessments of ACCELLION and its Accellion File Transfer Appliance to verify that  
22 ACCELLION and its Accellion File Transfer Appliance would comply with HIPAA privacy  
23 regulations and to follow guidelines and policies to maintain the privacy, confidentiality, including  
24 by encryption, and otherwise reasonably protect Plaintiff's and the Class' medical information from  
25 disclosure and/or release to at least one unauthorized third party "user" prior to and after TRINITY  
26 HEALTH's disclosure of and/or delivery of Plaintiff's and the Class members' medical information  
27 to ACCELLION and/or using its Accellion File Transfer Appliance.

28

32. For example, on January 12, 2021, ACCELLION issued a Press Release entitled “ACCELLION RESPONDS TO RECENT FTA SECURITY INCIDENT [-] Patch Released in 72 Hours with Minimal Impact” stating in part, “*In mid-December*, Accellion was made aware of a P0 vulnerability in its legacy File Transfer Appliance (FTA) software. Accellion FTA is a *20 year old product* that specializes in large file transfers. [¶] Accellion resolved the vulnerability and *released a patch within 72 hours to the less than 50 customers affected*. [¶] Accellion’s flagship enterprise content firewall platform, kiteworks, was not involved in any way. The kiteworks product has never reported an external P0 vulnerability during its four years in the marketplace.” (Emphasis added.) A copy of ACCELLION’s January 12, 2021 Press Release entitled “ACCELLION RESPONDS TO RECENT FTA SECURITY INCIDENT [-] Patch Released in 72 Hours with Minimal Impact” is attached hereto as **Exhibit B**.<sup>7</sup>

33. Additionally, on February 1, 2021, ACCELLION issued a Press Release entitled “ACCELLION PROVIDES UPDATE TO RECENT FTA SECURITY INCIDENT” stating in part, “*Accellion FTA, a 20 year old product nearing end-of life*, was the target of a sophisticated cyberattack. *All FTA customers were promptly notified of the attack on December 23, 2020*. At this time, Accellion has patched all known FTA vulnerabilities exploited by the attackers and has added new monitoring and alerting capabilities to flag anomalies associated with these attack vectors. [¶] All vulnerabilities are limited exclusively to FTA. They do not in any way impact Accellion’s enterprise content firewall platform known as kiteworks. The vast majority of Accellion’s clients reside on the kiteworks platform, which is built on an entirely different code base, using state-of-the-art security architecture, and a segregated, secure development process. [¶] In mid-December, Accellion was made aware of a zero-day vulnerability in its legacy FTA customers to mitigate the impact of the attack and to monitor for anomalies. [¶] ‘Our latest release of FTA has addressed all known vulnerabilities at this time,’ commented Frank Balonis, Accellion’s Chief Information Security Officer. “Future exploits, however, area constant threat. *We have encouraged all FTA customers to migrate to kiteworks for the last three years* and have

<sup>7</sup> (<https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/>, last visited May 19, 2021).

1 accelerated our FTA end-of-life plans in light of these attacks. We're main committed to assisting  
 2 our FTA customers, but strongly urge them to migrate to kiteworks as soon as possible.”  
 3 (Emphasis added.) A copy of ACCELLION's February 1, 2021 Press Release entitled  
 4 “ACCELLION PROVIDES UPDATE TO RECENT FTA SECURITY INCIDENT” is attached  
 5 hereto as **Exhibit C**.<sup>8</sup>

6 34. Additionally, on February 22, 2021, ACCELLION issued a Press Release entitled  
 7 “ACCELLION PROVIDES UPDATE TO RECENT FTA SECURITY INCIDENT FOLLOWING  
 8 MANDIANT PRLIMINARY FINDINGS” stating in part, “Mandiant, a division of FireEye, Inc.,  
 9 has identified UNC2546 as the criminal hacker behind the cyberattacks and data theft involving  
 10 Accellion's legacy File Transfer Appliance product. Multiple Accellion FTA customers who have  
 11 been attacked by UNC2546 have received extortion emails threatening to publish stolen data on the  
 12 “CL0P^ - LEAKS” .onion website. Some of the published victim data appears to have been stolen  
 13 using the DEWMODE web shell. Mandiant is tracking the subsequent extortion activity under a  
 14 separate threat cluster, UNC2582.”

15 35. Therefore, based upon TRINITY HEALTH's form letter, addressed to “Re: Patient,”  
 16 signed by Monica Lareau in her capacity as “Privacy Official,” attached hereto as **Exhibit A**, and  
 17 ACCELLION's Press Releases, attached hereto as **Exhibit B** and **Exhibit C**, Plaintiff alleges on  
 18 information and belief that *for the last three years*, ACCELLION encouraged TRINITY HEALTH  
 19 to migrate from *Accellion FTA, a 20 year old product nearing end-of life*, to its flagship enterprise  
 20 content firewall platform, kiteworks, which has never reported an external P0 vulnerability, and  
 21 TRINITY HEALTH negligently failed to do so, the negligent failure of which caused Plaintiff's and  
 22 the Class' medical information to be accessed, downloaded, stolen and viewed by at least one  
 23 unauthorized third party “user.” Additionally, based upon TRINITY HEALTH's form letter,  
 24 addressed to “Re: Patient,” signed by Monica Lareau in her capacity as “Privacy Official,” attached  
 25 hereto as **Exhibit A**, and ACCELLION's Press Releases, attached hereto as **Exhibit B** and **Exhibit**  
 26 **C**, Plaintiff alleges on information and belief that *on or about December 23, 2020 and prior to*  
 27 \_\_\_\_\_

28 <sup>8</sup> (<https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/>, last  
 visited May 19, 2021).

1 *January 20, 2021*, ACCELLION notified TRINITY HEALTH and released a patch to TRINITY  
2 HEALTH for installation in its Accellion File Transfer Appliance and TRINITY HEALTH  
3 negligently failed to install the patch to its Accellion File Transfer Appliance in a timely manner  
4 and prior to January 20, 2021, the negligent failure of which caused Plaintiff's and the Class'  
5 medical information to be accessed, downloaded, stolen and viewed by at least one unauthorized  
6 third party "user."

7 36. At all times relevant to this action, including the period prior to and on January 20,  
8 2021, at least one unauthorized third party "user" accessed and "downloaded" "certain files present  
9 on the [Accellion File Transfer] appliance on January 20[, 2021]" containing Plaintiff's and the  
10 Class' medical and "protected health information," including patients' names, addresses, email  
11 addresses, dates of birth, healthcare providers, dates and types of healthcare services, medical  
12 record numbers, immunization types, lab results, medications, payments, payer names and claims  
13 information, as determined by TRINITY HEALTH's investigation, in an un-encrypted format, as  
14 represented by TRINITY HEALTH in its form letter, addressed to "Re: Patient," signed by Monica  
15 Lareau in her capacity as "Privacy Official," attached hereto as **Exhibit A**. Thus, the cybercriminal  
16 accessed, downloaded and viewed Plaintiff's and the Class' un-encrypted medical information,  
17 including their names, addresses, email addresses, dates of birth, healthcare providers, dates and  
18 types of healthcare services, medical record numbers, immunization types, lab results, medications,  
19 payments, payer names and claims information, that, alone or in combination with other publicly  
20 available information, reveals their identity.

21 37. TRINITY HEALTH had the resources necessary to protect and preserve  
22 confidentiality of electronic medical information of Plaintiff and the Class in their possession, but  
23 neglected to adequately implement data security measures as required by HIPPA and the Act,  
24 despite their obligation to do so.

25 38. Additionally, the risk of vulnerabilities in its computer and data systems of being  
26 exploited by an unauthorized third party trying to steal Plaintiff's and the Class' electronic  
27 personally identifying and medical information was foreseeable and/or known to TRINITY  
28 HEALTH. The California Data Breach Report 2012-2015, issued in February 2016 by Attorney



1 General, Kamala D. Harris, reported, “Malware and hacking presents the greatest threat, both in the  
2 number of breaches and the number of records breached” and “Social Security numbers and  
3 medical information – was breached than other data types.” Moreover, as Attorney General further  
4 reported, just because “[e]xternal adversaries cause most data breaches, [] this does not mean that  
5 organizations are solely victims; they are also stewards of the data they collect and maintain. People  
6 entrust businesses and other organizations with their data on the understanding that the  
7 organizations have a both an ethical and a legal obligation to protect it from unauthorized access.  
8 Neglecting to secure systems and data opens a gateway for attackers, who take advantage of  
9 uncontrolled vulnerabilities.” Regarding encryption, Attorney General instructed in California Data  
10 Breach Report 2012-2015, “As we have said in the past, breaches of this type are preventable.  
11 Affordable solutions are widely available: strong full-disk encryption on portable devices and  
12 desktop computers when not in use.[] Even small businesses that lack full time information security  
13 and IT staff can do this. They owe it to their patients, customers, and employees to do it now.”

14 39. More recently the HIPAA Journal posted on November 1, 2018 warned, “Healthcare  
15 organization[s] need to ensure that their systems are well protected against cyberattacks, which  
16 means investing in technologies to secure the network perimeter, detect intrusions, and block  
17 malware and phishing threats.”

18 40. Further, it also was foreseeable and/or known to TRINITY HEALTH that  
19 negligently creating, maintaining, preserving, and/or storing Plaintiff’s and the Class’ medical and  
20 personal identifying information, in electronic form, in its Accellion File Transfer Appliance and in  
21 the email accounts of TRINITY HEALTH’s employees in a manner that did not preserve the  
22 confidentiality of the information could have a devastating effect on them. As reported in the  
23 California Data Breach Report 2012-2015, “There are real costs to individuals. Victims of a data  
24 breach are more likely to experience fraud than the general public, according to Javelin Strategy &  
25 Research. In 2014, 67 percent of breach victims in the U.S. were also victims of fraud, compared to  
26 just 25 percent of all consumers.”

27 41. To be successful, phishing relies on a series of affirmative acts by a company and its  
28 employees such as clicking a link, downloading a file, or providing sensitive information. Once



1 criminals gained access to the email accounts of a company and its employees, the email servers  
2 communicated—that is, disclosed—the contents of those accounts to the criminals. “Phishing  
3 scams are one of the most common ways hackers gain access to sensitive or confidential  
4 information. Phishing involves sending fraudulent emails that appear to be from a reputable  
5 company, with the goal of deceiving recipients into either clicking on a malicious link or  
6 downloading an infected attachment, usually to steal financial or confidential information.”  
7 (<https://www.varonis.com/blog/data-breach-statistics/>). As posted on April 21, 2020, the FBI had  
8 issued a fresh warning [Alert Number MI-000122-MW] following an increase in COVID-19  
9 phishing scams targeting healthcare providers.

10 42. At all times relevant to this action, including the period prior to and on January 20,  
11 2021, Defendants negligently created, maintained, preserved, and/or stored Plaintiff’s and the Class’  
12 medical information, including Plaintiff’s and the Class’ names, addresses, email addresses, dates of  
13 birth, healthcare providers, dates and types of healthcare services, medical record numbers,  
14 immunization types, lab results, medications, payments, payer names and claims information, in  
15 electronic form, onto Defendants’ email and computer network in a manner that did not preserve the  
16 confidentiality of the information, and negligently failed to protect and preserve confidentiality of  
17 electronic medical information of Plaintiff and the Class in their possession against unauthorized  
18 disclosure and/or release, including but not limited to, by failing to conduct and require adequate  
19 employee education and training, failing to adequately review & revise information security, failing  
20 to have adequate information security, and failing to have adequate privacy policies and procedures  
21 in place, as required by the Act, under Civil Code §§ 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a),  
22 56.101(b)(1)(A), and 56.36(e)(2)(E), and according to their written representations to Plaintiff and  
23 the Class.

24 43. Had TRINITY HEALTH and/or its employees (presently unknown to Plaintiff)  
25 taken such appropriate preventive actions, fix the deficiencies in their Accellion File Transfer  
26 Appliance, email accounts, email and computer network, and data security systems, and adopted  
27 security measures as required by HIPPA and the Act prior to and on January 20, 2021, TRINITY  
28 HEALTH could have prevented Plaintiff’s and the Class’ electronic medical information in their

1 Accellion File Transfer Appliance and in the email accounts of TRINITY HEALTH's employees  
2 from being accessed, downloaded, stolen and viewed by at least one unauthorized third party  
3 "user."

4 44. On and before January 20, 2021, TRINITY HEALTH and/or its employees  
5 (presently unknown to Plaintiff), by negligently creating, maintaining, preserving, and storing the  
6 electronic medical information of Plaintiff and the Class in their Accellion File Transfer Appliance  
7 and in one or more of and the email accounts of its employees, allowed Plaintiff's and the Class'  
8 individually identifiable medical information to be accessed, downloaded, stolen and viewed by at  
9 least one unauthorized third party "user," without first obtaining an authorization, constituting a  
10 disclosure in violation of Civil Code §§ 56.10(a), 56.13, 56.245 and 56.26(a).

11 45. On and before January 20, 2021, TRINITY HEALTH and/or its employees  
12 (presently unknown to Plaintiff), by negligently creating, maintaining, preserving, and storing the  
13 electronic medical information of Plaintiff and the Class in their Accellion File Transfer Appliance  
14 and in one or more of the email accounts of its employees, allowed Plaintiff's and the Class'  
15 individually identifiable medical information to be accessed, downloaded, stolen and viewed by at  
16 least one unauthorized third party "user," constituting a release in violation of Civil Code §  
17 56.101(a).

18 46. On and before January 20, 2021, TRINITY HEALTH and/or its employees  
19 (presently unknown to Plaintiff), by negligently creating, maintaining, preserving, and storing the  
20 electronic medical information of Plaintiff and the Class in their Accellion File Transfer Appliance  
21 and in one or more of the email accounts of its employees, allowed Plaintiff's and the Class'  
22 individually identifiable medical information to be accessed, downloaded, stolen and viewed by at  
23 least one unauthorized third party "user," constituting a release in violation of Civil Code §  
24 56.101(a).

25 47. On and before January 20, 2021, TRINITY HEALTH's and/or its employees'  
26 negligent failure to protect and preserve confidentiality of electronic medical information of  
27 Plaintiff and the Class in their Accellion File Transfer Appliance and in one or more of the email  
28 accounts of its employees, allowed Plaintiff's and the Class' individually identifiable medical

1 information to be accessed, downloaded, stolen and viewed by at least one unauthorized third party  
2 “user,” constituting a release in violation of Civil Code § 56.101(b)(1)(A).

3 48. California law requires a business to notify any California resident whose  
4 unencrypted personal information, as defined, was acquired, or reasonably believed to have been  
5 acquired, by an unauthorized person. California law also requires that a sample copy of a breach  
6 notice sent to more than 500 California residents must be provided to the California Attorney  
7 General. On or about April 6, 2021, TRINITY HEALTH caused a form letter sent on its behalf,  
8 addressed to “Re: Patient,” signed by Monica Lareau in her capacity as “Privacy Official” of  
9 TRINITY HEALTH, an exemplar of which is attached hereto as **Exhibit A**, to be submitted to the  
10 Attorney General of the State of California and to be mailed to Plaintiff and the Class, stating in  
11 part, “because the patient listed above receives service from a hospital or health care provider that  
12 is a current or former member of Trinity Health,” and informing her, in part, of “an incident that  
13 may impact the privacy of certain confidential information related to the patient. Trinity Health was  
14 recently notified by Accellion, a third-party vendor, of a security incident. The Accellion File  
15 Transfer Appliance is used by Trinity Health and many other companies for large file transfer  
16 service.... **What Happened?** On January 29, 2021, Accellion informed Trinity Health of a security  
17 issue with its secure file transfer platform, used for sending secure email. Upon receiving this  
18 notice, Trinity Health ... launched an investigation into the issue and its impact on both Trinity  
19 Health and our patients and colleagues. This investigation determined that certain files present on  
20 the appliance on January 20 were downloaded by an unknown user.... **What Information is**  
21 **Involved?** Although the investigation is ongoing, on February 4, 2021, we determined file(s) were  
22 present on the appliance at the time of this event. The files contained certain protected health  
23 information, including some combination of the **following patient’s name, address, email, date of**  
24 **birth, healthcare provider, dates and types of healthcare services, medical record number,**  
25 **immunization type, lab results, medications, payment, payer name and claims information.”**  
26 Further, because TRINITY HEALTH submitted its form letter to the Attorney General of the State  
27 of California and mailed it to Plaintiff and the Class, TRINITY HEALTH concedes that Plaintiff’s  
28 and the Class’ identifiable medical information contained in TRINITY HEALTH’s Accellion File

1 Transfer Appliance and in one or more of the email accounts of TRINITY HEALTH's employees  
2 was unencrypted and thus, the unauthorized third party or parties who accessed and "downloaded"  
3 Plaintiff's and the Class' identifiable medical information was able to and did actually view  
4 Plaintiff's and the Class' electronic medical information contained in and "downloaded" from  
5 TRINITY HEALTH's email and computer network, TRINITY HEALTH's Accellion File Transfer  
6 Appliance, and one or more of the email accounts of TRINITY HEALTH's employees. As a result,  
7 TRINITY HEALTH was negligent for failing to encrypt or adequately encrypt Plaintiff's and the  
8 Class' electronic medical information contained in its email and computer network, its Accellion  
9 File Transfer Appliance, and one or more of the email accounts of its employees.

10 49. TRINITY HEALTH's form letter submitted to the Attorney General of the State of  
11 California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**, further states,  
12 "Trinity Health is also offering the patient complimentary access to credit monitoring services as  
13 appropriate to the information impacted."

14 50. TRINITY HEALTH's form letter submitted to the Attorney General of the State of  
15 California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**, concludes by making  
16 the following hollow gesture, "We apologize for any inconvenience or concern this situation may  
17 have caused you." Other than offering its "apolog[y]" and "identity monitoring at no cost to you for  
18 one year," TRINITY HEALTH's form letter does nothing to further protect Plaintiff and the Class  
19 from future incidents of identity theft despite the severity of the unauthorized access, viewing,  
20 exfiltration, theft, disclosure and release of their electronic medical and personal information caused  
21 by TRINITY HEALTH's violations of its duty to implement and maintain reasonable security  
22 procedures and practices. To date, other than offering its "apolog[y]" and "identity monitoring at no  
23 cost to you for one year," TRINITY HEALTH has not offered any monetary compensation for the  
24 unauthorized disclosure and/or release of Plaintiff's and the Class' electronic medical information  
25 under the Act. In effect, TRINITY HEALTH is shirking its responsibility for the harm it has  
26 caused, while shifting the burdens and costs of its wrongful conduct onto its patients, i.e. Plaintiff  
27 and the Class.

1           51. Based upon the information posted on the U.S. Department of Health and Human  
2 Services' official website, TRINITY HEALTH reported on "04/05/2021" a "Hacking/IT Incident"  
3 involving "Network Server" affecting "586,869" persons, which involved a "Business Associate,"  
4 to the U.S. Department of Health & Human Services' Office for Civil Rights.

5           52. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA  
6 covered entities to provide notification following a breach of unsecured protected health  
7 information. Following a breach of unsecured protected health information, covered entities must  
8 provide notification of the breach to affected individuals. Covered entities must *only* provide the  
9 required notifications if the breach involved unsecured protected health information. Unsecured  
10 protected health information is protected health information (PHI) that has not been rendered  
11 unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or  
12 methodology specified by the Secretary of the U.S. Department of Health and Human Services in  
13 guidance. Under approved guidance of the U.S. Department of Health and Human Services, PHI is  
14 rendered unusable, unreadable, or indecipherable to unauthorized individuals if (1) electronic PHI  
15 has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process  
16 to transform data into a form in which there is a low probability of assigning meaning without use  
17 of a confidential process or key" (45 CFR 164.304 definition of encryption) and (2) such  
18 confidential process or key that might enable decryption has not been breached. By reporting this  
19 incident to the U.S. Department of Health and Human Services, TRINITY HEALTH has  
20 determined and is conceding that the Class' electronic PHI was either not encrypted at all, or if it  
21 was encrypted, the encryption has been breached by the unauthorized third party. As a result,  
22 TRINITY HEALTH concedes that Plaintiff's and the Class' identifiable medical information  
23 contained in TRINITY HEALTH's Accellion File Transfer Appliance and in one or more of the  
24 email accounts of TRINITY HEALTH's employees was unencrypted and thus, the unauthorized  
25 third party or parties who accessed and "downloaded" Plaintiff's and the Class' identifiable medical  
26 information was able to and did actually view Plaintiff's and the Class' electronic medical  
27 information contained in and "downloaded" from TRINITY HEALTH's email and computer  
28 network, TRINITY HEALTH's Accellion File Transfer Appliance, and one or more of the email

accounts of TRINITY HEALTH's employees. Therefore, TRINITY HEALTH was negligent for failing to encrypt or adequately encrypt Plaintiff's and the Class' electronic medical information contained in their Accellion File Transfer Appliance and in one or more of the email accounts of its employees. Further, because Plaintiff's and the Class' identifiable medical information contained in TRINITY HEALTH's Accellion File Transfer Appliance and in one or more of the email accounts of TRINITY HEALTH's employees was not rendered unusable, unreadable, or indecipherable, the unauthorized third party or parties who accessed and "downloaded" Plaintiff's and the Class' identifiable medical information was able to and did actually view Plaintiff's and the Class' electronic medical information contained in and "downloaded" from TRINITY HEALTH's email and computer network, TRINITY HEALTH's Accellion File Transfer Appliance, and one or more of the email accounts of TRINITY HEALTH's employees.

#### **CLASS ACTION ALLEGATIONS**

53. Plaintiff brings this action on behalf of herself individually and on behalf of all others similarly situated. The putative class that Plaintiff seeks to represent is defined as follows:

Class: All persons to whom Trinity Health Corporation sent a notification letter of a data security incident that occurred on January 20, 2021, an exemplar of which is attached hereto as **Exhibit A**.

The officers, directors, and employees of TRINITY HEALTH are excluded from the Class. The officers, directors, and employees of any "affiliate," "principal" and "subsidiary" of TRINITY HEALTH, as defined in the Corporations Code §§ 150, 175, and 189, respectively, are excluded from the Class. Plaintiff reserves the right under California Rule of Court 3.765 to amend or modify the Class definition with greater particularity or further division into subclasses or limitation to particular issues as warranted, and as additional facts are discovery by Plaintiff during her future investigations.

54. This action is properly maintainable as a class action. The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. While the exact number of the Class members is unknown to Plaintiff at this time, TRINITY HEALTH filed a



1 report with the U.S. Department of Health & Human Services' Office for Civil Rights, on or about  
2 April 5, 2021, that this security incident affected 586,869 persons. The disposition of the claims of  
3 the members of Class through this class action will benefit both the parties and this Court. In  
4 addition, the Class is readily identifiable from information and records in the possession of  
5 TRINITY HEALTH and its agents, and the Class is defined in objective terms that make the  
6 eventual identification of Class members possible and/or sufficient to allow members of the Class to  
7 identify themselves as having a right to recover.

8 55. There is a well-defined community of interest among the members of the Class  
9 because common questions of law and fact predominate, Plaintiff's claims are typical of the  
10 members of the Class, and Plaintiff can fairly and adequately represent the interests of the Class.

11 56. Common questions of law and fact exist as to all members of the Class and the Class  
12 and predominate over any questions affecting solely individual members of the Class and the Class.  
13 Among the questions of law and fact common to the Class that predominate over questions which  
14 may affect individual Class members, including the following:

- 15 a) Whether Defendants possessed Plaintiff's and the Class' medical and personal  
16 identifying information prior to and on January 20, 2021;
- 17 b) Whether Defendants created, maintained, preserved and/or stored Plaintiff's and the  
18 Class' medical and personal identifying information, in electronic form, onto  
19 Defendants' email and computer network prior to and on January 20, 2021;
- 20 c) Whether Defendants implemented and maintained reasonable security procedures  
21 and practices to protect Plaintiff's and the Class' medical and personal identifying  
22 information, in electronic form, within Defendants' email and computer network  
23 prior to and on January 20, 2021;
- 24 d) Whether Plaintiff's and the Class' medical and personal identifying information, in  
25 electronic form, within Defendants' email and computer network prior to and on  
26 January 20, 2021 was accessed, viewed, exfiltrated and/or publicly exposed by an  
27 unauthorized third party;



- e) Whether Plaintiff's and the Class' medical and personal identifying information, in electronic form, within Defendants' email and computer network prior to and on January 20, 2021 was accessed, viewed, exfiltrated and/or publicly exposed by an unauthorized third party without the prior written authorization of Plaintiff and the Class, as required by Civil Code §§ 56.10 and 56.26;
- f) Whether Defendants' creation, maintenance, preservation and/or storage of Plaintiff's and the Class' medical and personal identifying information, in electronic form, within Defendants' email and computer networks, accessed, viewed, exfiltrated and/or publicly exposed by an unauthorized third party was permissible without written authorization from Plaintiff and the Class or under any exemption under Civil Code § 56.10(c);
- g) Whether Defendants' creation, maintenance, preservation and/or storage of Plaintiff's and the Class' medical and personal identifying information, in electronic form, within Defendants' email and computer network, accessed, viewed, exfiltrated and/or publicly exposed by an unauthorized third party constitutes a release in violation of Civil Code §56.101;
- h) Whether the timing of Defendants' notice that Plaintiff's and the Class' medical and personal identifying information, in electronic form, was accessed, viewed, exfiltrated and/or publicly exposed by an unauthorized third party, was given in the most expedient time possible and without reasonable delay;
- i) Whether Defendants' conduct constitute unlawful, fraudulent or unfair practices in violation of Business and Professions Code §§ 17200, *et seq.*; and
- j) Whether Plaintiff and the Class are entitled to actual, nominal or statutory damages, injunctive relief and/or restitution.

57. Plaintiff's claims are typical of those of the other Class members because Plaintiff, like every other Class member, was exposed to virtually identical conduct and now suffer from the same violations of the law as other Class members.

1        58. Plaintiff will fairly and adequately protect the interests of the Class. Moreover,  
2 Plaintiff has no interest that is contrary to or in conflict with those of the Class she seeks to  
3 represent. In addition, Plaintiff has retained competent counsel experienced in class action litigation  
4 to further ensure such protection and intend to prosecute this action vigorously.

5        59. The nature of this action and the nature of laws available to Plaintiff and the  
6 members of Class make the use of the class action format a particularly efficient and appropriate  
7 procedure to afford relief to Plaintiff and Class for the claims alleged and the disposition of whose  
8 claims in a class action will provide substantial benefits to both the parties and the Court because:

- 9            a) If each member of the Class were required to file an individual lawsuit, TRINITY  
10            HEALTH would necessarily gain an unconscionable advantage since they would be  
11            able to exploit and overwhelm the limited resources of each individual member of  
12            the Class with its vastly superior financial and legal resources;
- 13            b) The costs of individual suits could unreasonably consume the amounts that would be  
14            recovered;
- 15            c) Proof of a common business practice or factual pattern which Plaintiff experienced is  
16            representative of that experienced by the Class and will establish the right of each of  
17            the members to recover on the causes of action alleged;
- 18            d) Individual actions would create a risk of inconsistent results and would be  
19            unnecessary and duplicative of this litigation;
- 20            e) TRINITY HEALTH has acted or refused to act on grounds generally applicable to  
21            the Class as a whole, thereby making it appropriate to render judgment with respect  
22            to the Class as a whole in this litigation; and
- 23            f) The disposition of the claims of the members of Class through this class action will  
24            produce salutary by-products, including a therapeutic effect upon those who indulge  
25            in unlawful practices, and aid to legitimate business enterprises by curtailing  
26            unlawful competition.

27        60. The prosecution of separate actions by individual members of the Class would create  
28 a risk of inconsistent or varying adjudications with respect to individual members of the Class,

1 which would establish incompatible standards of conduct for the Defendants in the State of  
2 California and would lead to repetitious trials of the numerous common questions of fact and law in  
3 the State of California. Plaintiff knows of no difficulty that will be encountered in the management  
4 of this litigation that would preclude its maintenance as a class action. As a result, a class action is  
5 superior to other available methods for the fair and efficient adjudication of this controversy.

6 61. Notice to the members of the Class may be made by e-mail or first-class mail  
7 addressed to all persons who have been individually identified by Defendants and who have been  
8 given notice of the data breach.

9 62. Plaintiff and the Class have suffered irreparable harm and damages because of  
10 Defendants' wrongful conduct as alleged herein. Absent certification, Plaintiff and the Class will  
11 continue to be damaged and to suffer by the unauthorized disclosure and/or release of their medical  
12 and personal identifying information, thereby allowing these violations of law to proceed without  
13 remedy.

14 63. Moreover, Plaintiff's and the Class' individual damages are insufficient to justify the  
15 cost of litigation, so that in the absence of class treatment, Defendants' violations of law inflicting  
16 substantial damages in the aggregate would go unremedied. In addition, Defendants have acted or  
17 refused to act on grounds generally applicable to Plaintiff and the Class, thereby making appropriate  
18 final injunctive relief with respect to, the Class as a whole.

19 **FIRST CAUSE OF ACTION**  
20 **Violations of the Confidentiality of Medical Information Act**  
21 **California Civil Code §§ 56, et seq.**  
22 **(On Behalf of Plaintiff and the Class All Defendants)**

23 64. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if  
24 fully stated herein.

25 65. At all times relevant to this action, including on and before January 20, 2021,  
26 Defendants are providers of health care, contractors, and/or other authorized recipients of personal  
27 and confidential medical information as defined and set forth in the California Confidentiality of  
28 Medical Information Act, California Civil Code §§ 56, *et seq.* (the "Act") and maintained and

1 continues to maintain “medical information,” within the meaning of Civil Code § 56.05(j), of  
2 Plaintiff and other “patients” within the meaning of Civil Code § 56.05(k).

3         66. At all times relevant to this action, including on and before January 20, 2021,  
4 Defendants lawfully came into possession of Plaintiffs’ and Class members’ personally identifiable  
5 medical information, including the names, addresses, email addresses, dates of birth, healthcare  
6 providers, dates and types of healthcare services, medical record numbers, immunization types, lab  
7 results, medications, payments, payer names and claims information of Plaintiff and the Class, and  
8 had a duty to exercise reasonable care in preserving the confidentiality of this information subject to  
9 the requirements and mandates of the Act, including but not limited to Civil Code §§ 56.10, 56.13,  
10 56.245, 56.26, 56.101 and 56.36. At all times relevant to this action, including on and before  
11 January 20, 2021, Plaintiff and the Class had their individually identifiable “medical information,”  
12 within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored in  
13 TRINITY HEALTH’s email and computer network, in TRINITY HEALTH’s Accellion File  
14 Transfer Appliance, and in the email accounts of TRINITY HEALTH’s employees. Further, at all  
15 times relevant to this action, including on and before January 20, 2021, Plaintiff and the Class are  
16 “patients” within the meaning of Civil Code § 56.05(k), and are “Endanger” within the meaning of  
17 Civil Code § 56.05(e) because they fear that disclosure and/or release of their medical information  
18 could subject them to harassment or abuse.

19         67. As a result, at all times relevant to this action, including on and before January 20,  
20 2021, Defendants and/or unknown employees negligently created, maintained, preserved, and/or  
21 stored Plaintiff’s and the Class’ individual identifiable “medical information,” within the meaning  
22 of Civil Code § 56.05(j), including Plaintiff’s and Class members’ names, addresses, email  
23 addresses, dates of birth, healthcare providers, dates and types of healthcare services, medical  
24 record numbers, immunization types, lab results, medications, payments, payer names and claims  
25 information, in TRINITY HEALTH’s email and computer network, in TRINITY HEALTH’s  
26 Accellion File Transfer Appliance, and in the email accounts of TRINITY HEALTH’s employees  
27 in a manner that did not preserve the confidentiality of the information, and negligently failed to  
28 protect and preserve confidentiality of electronic medical information of Plaintiff and the Class in

1 its possession against disclosure and/or release, including but not limited to, by failing to conduct  
2 and require adequate employee education and training, failing to adequately review & revise  
3 information security, failing to have adequate information security, and failing to have adequate  
4 privacy policies and procedures in place, as required by the Act, under Civil Code §§ 56.10(a),  
5 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and 56.36(e)(2)(E).

6 68. Due to TRINITY HEALTH's and/or its employees' negligent creation, maintenance,  
7 preservation and/or storage of Plaintiff's and the Class' electronic medical information in TRINITY  
8 HEALTH's email and computer network, in TRINITY HEALTH's Accellion File Transfer  
9 Appliance, and in the email accounts of TRINITY HEALTH's employees, TRINITY HEALTH  
10 allowed Plaintiff's and the Class' individually identifiable medical information to be accessed and  
11 actually viewed by at least one unauthorized third party on or before January 20, 2021, without first  
12 obtaining an authorization within the meaning of Civil Code § 56.05(a), constituting a disclosure in  
13 violation of Civil Code §§ 56.10, 56.13, 56.245, and 56.26(a).

14 69. Due to TRINITY HEALTH's and/or its employees' negligent creation,  
15 maintenance, preservation and/or storage of Plaintiff's and the Class' electronic medical  
16 information in TRINITY HEALTH's email and computer network, in TRINITY HEALTH's  
17 Accellion File Transfer Appliance, and in the email accounts of TRINITY HEALTH's employees,  
18 TRINITY HEALTH allowed Plaintiff's and the Class' individually identifiable medical information  
19 to be accessed and actually viewed by at least one unauthorized third party on or before January 20,  
20 2021, constituting a release in violation of Civil Code § 56.101(a).

21 70. Due to TRINITY HEALTH's and/or its employees' negligent creation, maintenance,  
22 preservation and/or storage of Plaintiff's and the Class' electronic medical information in TRINITY  
23 HEALTH's email and computer network, in TRINITY HEALTH's Accellion File Transfer  
24 Appliance, and in the email accounts of TRINITY HEALTH's employees, TRINITY HEALTH  
25 allowed Plaintiff's and the Class' individually identifiable medical information to be accessed and  
26 actually viewed by at least one unauthorized third party on or before January 20, 2021, constituting  
27 a release in violation of Civil Code § 56.101(b)(1)(A).

28

71. As a result of TRINITY HEALTH's and/or its employees' above-described conduct in violation of the Act, Plaintiff and the Class have suffered damages from the unauthorized disclosure and/or release of their individual identifiable medical information.

72. As a direct and proximate result of TRINITY HEALTH's and/or its employees' above-described conduct in violation of the Act, Plaintiff and the Class are entitled to recover, "against any person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both of the following: (1) ... nominal damages of one thousand dollars (\$1,000). In order to recover under this paragraph, it shall not be necessary that the plaintiff suffered or was threatened with actual damages. (2) The amount of actual damages, if any, sustained by the patient."

73. As a result of TRINITY HEALTH's and/or its employees' above-described conduct in violation of the Act, Plaintiff and the Class seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil Code § 56.36(b)(2) from all Defendants.

**SECOND CAUSE OF ACTION**  
**Breach of California Security Notification Laws**  
**California Civil Code § 1798.82**  
**(On Behalf of Plaintiff and the Class Against All Defendants)**

74. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if fully stated herein.

75. Pursuant to Civil Code § 1798.82(a), "A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that

1 personal information readable or usable. The disclosure shall be made in the most expedient time  
2 possible and without unreasonable delay, consistent with the legitimate needs of law enforcement,  
3 as provided in subdivision (c), or any measures necessary to determine the scope of the breach and  
4 restore the reasonable integrity of the data system.” Prior to passage of such statute, the California  
5 State Assembly cited an incident where authorities knew of the breach in security for 21 days  
6 “before state workers were told” as an example of “late notice.”

7 76. Civil Code § 1798.82 further provides, “(h) For purposes of this section, ‘personal  
8 information’ means an individual’s first name or first initial and last name in combination with any  
9 one or more of the following data elements, when either the name or the data elements are not  
10 encrypted: (1) Social security number. (2) Driver’s license number or California Identification Card  
11 number. (3) Account number, credit or debit card number, in combination with any required  
12 security code, access code, or password that would permit access to an individual’s financial  
13 account. (4) Medical information. (5) Health insurance information. (i) .... (2) For purposes of this  
14 section, ‘medical information’ means any information regarding an individual’s medical history,  
15 mental or physical condition, or medical treatment or diagnosis by a health care professional. (3)  
16 For purposes of this section, ‘health insurance information’ means an individual’s health insurance  
17 policy number or subscriber identification number, any unique identifier used by a health insurer to  
18 identify the individual, or any information in an individual’s application and claims history,  
19 including any appeals records.”

20 77. TRINITY HEALTH conducts business in California and owns or licenses  
21 computerized data which includes the personal information, within the meaning of Civil Code §  
22 1798.82(h), of Plaintiff and the Class.

23 78. Based upon TRINITY HEALTH’s form letter submitted to the Attorney General of  
24 the State of California and mailed to Plaintiff and the Class attached hereto as **Exhibit A**, TRINITY  
25 HEALTH was aware that Plaintiff’s and the Class’ unencrypted personal information was, or is  
26 reasonably believed to have been, acquired by an unauthorized person no later than February 4,  
27 2021, but did not begin to mail notification letters to Plaintiff and the Class until April 6, 2021.  
28 Thus, TRINITY HEALTH waited at least 62 days before *beginning* to inform Plaintiff and the



1 Class of this incident and the subsequent threat to Plaintiff's and the Class' unencrypted personal  
2 information. As a result, TRINITY HEALTH did not disclose to Plaintiff and the Class that their  
3 unencrypted personal information was, or was reasonably believed to have been, acquired by an  
4 unauthorized person, in the most expedient time possible and without reasonable delay in violation  
5 of Civil Code § 1798.82(a). Given the example of the Legislature finding that a delay of 21 days to  
6 be "late notice" under the statute, TRINITY HEALTH's delay of 62 days before *beginning* to  
7 inform Plaintiff and the Class that their personal information was, or was reasonably believed to  
8 have been, acquired by an unauthorized person by mailing TRINITY HEALTH's form letter to  
9 Plaintiff and the Class is presumptively unreasonable notice in violation of Civil Code § 1798.82(a).

10 79. Upon information and belief, Plaintiff believes and alleges that no law enforcement  
11 agency has notified Defendants that the notification would impede a criminal investigation  
12 justifying TRINITY HEALTH's decision to wait 62 days *before beginning to mail* notification  
13 letters to Plaintiff and the Class *after* they knew that Plaintiff's and the Class' unencrypted personal  
14 information on TRINITY HEALTH's email and computer server was, or was reasonably believed  
15 to have been, acquired by an unauthorized person. Upon information and belief, Plaintiff believes  
16 and alleges that there were no measures taken by TRINITY HEALTH to determine the scope of the  
17 breach or to restore the reasonable integrity of the data system, which justifies TRINITY  
18 HEALTH's decision to wait 62 days *before beginning to mail* notification letters to Plaintiff and the  
19 Class. Moreover, TRINITY HEALTH's notification letter mailed to Plaintiff and the Class failed to  
20 be titled "Notice of Data Breach," in violation of Civil Code § 1798.82(d)(1), and failed to state  
21 whether notification was delayed as a result of a law enforcement investigation, in violation of Civil  
22 Code § 1798.82(d)(2)(D).

23 80. Plaintiff and the Class have been injured by fact that Defendants did not disclose to  
24 them that their unencrypted personal information was, or was reasonably believed to have been,  
25 acquired by an unauthorized person in the most expedient time possible and without reasonable  
26 delay in violation of Civil Code § 1798.82(a). Defendants' delays in informing required by Civil  
27 Code § 1798.82(a) and providing all of the information required by Civil Code § 1798.82(d) to  
28 Plaintiff and the Class that their unencrypted personal information was, or was reasonably believed

1 to have been, acquired by an unauthorized person, have prevented Plaintiff and the Class from  
2 taking steps in the most expedient time possible to protect their unencrypted personal information  
3 from unauthorized use and/or identify theft.

4 81. Plaintiff and the Class seek recovery of their damages pursuant to Civil Code §  
5 1798.84(b) and injunctive relief pursuant to Civil Code § 1798.84(e) from all Defendants.

6 **THIRD CAUSE OF ACTION**  
7 **Unlawful and Unfair Business Acts and Practices in Violation of**  
8 **California Business & Professions Code §17200, *et seq.***  
9 **(On Behalf of Plaintiff and the Class Against All Defendants)**

10 82. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if  
11 fully stated herein.

12 83. The acts, misrepresentations, omissions, practices, and non-disclosures of  
13 Defendants as alleged herein constituted unlawful and unfair business acts and practices within the  
14 meaning of California Business & Professions Code §§ 17200, *et seq.*

15 84. By the aforementioned business acts or practices, Defendants have engaged in  
16 “unlawful” business acts and practices in violation of the aforementioned statutes, including Civil  
17 Code §§ 56.10(a), 56.26(a), 56.36(e)(2)(E), 56.101(a), 56.101(b)(1)(A), 1798.82(a) and 1798.82(d).  
18 Plaintiff reserves the right to allege other violations of law committed by Defendants which  
19 constitute unlawful acts or practices within the meaning of California Business & Professions Code  
20 §§ 17200, *et seq.*

21 85. By the aforementioned business acts or practices, Defendants have also engaged in  
22 “unfair” business acts or practices in that the harm caused by Defendants’ failure to maintain  
23 adequate information security procedures and practices, including but not limited to, failing to take  
24 adequate and reasonable measures to ensure its data systems were protected against unauthorized  
25 intrusions, failing to properly and adequately educate and train its employees, failing to put into  
26 place reasonable or adequately computer systems and security practices to safeguard patients’  
27 identifiable medical information including access restrictions and encryption, failing to have  
28 adequate privacy policies and procedures in place that did not preserve the confidentiality of the  
medical and personal identifying information of Plaintiff and the Class in their possession, and

1 failing to protect and preserve confidentiality of electronic medical information of Plaintiff and the  
2 Class in their possession against disclosure and/or release, outweighs the utility of such conduct and  
3 such conduct offends public policy, is immoral, unscrupulous, unethical, deceitful and offensive,  
4 and causes substantial injury to Plaintiff and the Class.

5 86. Defendants have obtain money and property from Plaintiff and the Class because of  
6 the payment of the services and products they received from Defendants. Plaintiff and the Class  
7 have suffered an injury in fact by acquiring less in their transactions with Defendants for the  
8 services and products they received from Defendants than they otherwise would have if Defendants  
9 would had adequately protected the confidentiality of their medical and personal identifying  
10 information.

11 87. Pursuant to the Business & Professions Code § 17203, Plaintiff and the Class seek an  
12 order of this Court requiring Defendants awarding Plaintiff and the Class restitution of monies  
13 wrongfully acquired by Defendants in the form of payments for services by means of such  
14 unlawful, fraudulent and unfair business acts and practices, so as to restore any and all monies to  
15 Plaintiff and the Class which were acquired and obtained by means of such unlawful, fraudulent and  
16 unfair business acts and practices, which ill-gotten gains are still retained by Defendants.

17 88. The aforementioned unlawful, fraudulent and unfair business acts or practices  
18 conducted by Defendants have been committed in the past and continues to this day. Defendants  
19 have failed to acknowledge the wrongful nature of their actions. Defendants have not corrected or  
20 publicly issued comprehensive corrective notices to Plaintiff and the Class, and have not corrected  
21 or enacted adequate privacy policies and procedures to protect and preserve confidentiality of  
22 medical and personal identifying information of Plaintiff and the Class in their possession.

23 89. Because of Defendants' aforementioned conduct, Plaintiff and the Class have no  
24 other adequate remedy of law in that absent injunctive relief from the Court and Defendants are  
25 likely to continue to injure Plaintiff and the Class.

26 90. Pursuant to Business & Professions Code § 17203, Plaintiff and the Class also seek  
27 an order of this Court for equitable and/or injunctive relief in the form of requiring Defendants to  
28 correct its illegal conduct that is necessary and proper to prevent Defendants from repeating their

1 illegal and wrongful practices as alleged above and protect and preserve confidentiality of medical  
2 and personal identifying information of Plaintiff and the Class in Defendants' possession that has  
3 already been accessed, downloaded, exfiltrated, stolen and viewed by at least one unauthorized third  
4 party because by way of Defendants' illegal and wrongful practices set forth above. Pursuant to  
5 Business & Professions Code § 17203, Plaintiff and the Class further seek an order of this Court for  
6 equitable and/or injunctive relief in the form of requiring Defendants to publicly issue  
7 comprehensive corrective notices.

8 91. Because this case is brought for the purposes of enforcing important rights affecting  
9 the public interest, Plaintiff and the Class also seek the recovery of attorneys' fees and costs in  
10 prosecuting this action against Defendants under Code of Civil Procedure § 1021.5 and other  
11 applicable law.

12 **PRAYER FOR RELIEF**

13 WHEREFORE, Plaintiff respectfully request that the Court grant Plaintiff and the proposed  
14 Class the following relief against Defendants, and each of them:

15 **As for the First Cause of Action**

- 16 1. For nominal damages in the amount of one thousand dollar (\$1,000) per violation to Plaintiff  
17 individually and to each member of the Class and the Class pursuant to Civil Code §  
18 56.36(b)(1);  
19 2. For actual damages according to proof per violation pursuant to Civil Code § 56.36(b)(2);

20 **As for the Second Cause of Action**

- 21 3. For damages according to proof to Plaintiff individually and to each member of the Class  
22 and the Class pursuant to California Civil Code § 1798.84(b);  
23 4. For injunctive relief pursuant to California Civil Code § 1798.84(e);

24 **As for the Third Cause of Action**

- 25 5. For an order awarding Plaintiff and the Class restitution of all monies wrongfully acquired  
26 by Defendants by means of such unlawful, fraudulent and unfair business acts and practices;  
27 6. For injunctive relief in the form of an order instructing Defendants to prohibit the  
28 unauthorized release of medical and personal identifying information of Plaintiff and the

1 Class, and to adequately maintain the confidentiality of the medical and personal identifying  
2 information of Plaintiff and the Class;

- 3 7. For injunctive relief in the form of an order enjoining Defendants from disclosing the  
4 medical and personal identifying information of Plaintiff and the Class without the prior  
5 written authorization of each Plaintiff and the Class member;

6 **As to All Causes of Action**

- 7 8. That the Court issue an Order certifying this action be certified as a class action on behalf of  
8 the proposed Class, appointing Plaintiff as representative of the proposed Class, and  
9 appointing Plaintiff's attorneys, as counsel for members of the proposed Class;
- 10 9. For an award of attorneys' fees as authorized by statute, including, but not limited to, the  
11 provisions of California Code of Civil Procedure § 1021.5, and as authorized under the  
12 "common fund" doctrine, and as authorized by the "substantial benefit" doctrine;
- 13 10. For costs of the suit;
- 14 11. For prejudgment interest at the legal rate; and
- 15 12. Any such further relief as this Court deems necessary, just, and proper.

16 Dated: May 20, 2021

KEEGAN & BAKER LLP

17  
18 By:


  
Patrick N. Keegan, Esq.  
Attorney for Plaintiff

**DEMAND FOR JURY TRIAL**

Plaintiff and the Class hereby demand a jury trial on all causes of action and claims with respect to which they have a right to jury trial.

Dated: May 20, 2021

**KEEGAN & BAKER LLP**

By:   
Patrick N. Keegan, Esq.  
Attorney for Plaintiff

# Exhibit A





Membership #: &lt;&lt;Member ID&gt;&gt;

Call center (855) 935-6070

&lt;&lt;Date&gt;&gt; (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
 <<address\_1>>  
 <<address\_2>>  
 <<city>>, <<state\_province>> <<postal\_code>>  
 <<country >>

Re: Patient: &lt;&lt;first\_name&gt;&gt; &lt;&lt;middle\_name&gt;&gt; &lt;&lt;last\_name&gt;&gt; &lt;&lt;suffix&gt;&gt;,

You are receiving this letter because the patient listed above receives service from a hospital or health care provider that is a current or former member of Trinity Health\*. The purpose of this letter is to notify you of an incident that may impact the privacy of certain confidential information related to the patient. Trinity Health was recently notified by Accellion, a third-party vendor, of a security incident. The Accellion File Transfer Appliance is used by Trinity Health and many other companies for large file transfer service. Trinity Health provides information technology services for its current and some former member hospitals and health care providers, including file transfer and email services (\* please see included information about Trinity Health and the affected locations).

This letter provides you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so. While we are unaware of misuse of information, we encourage you to remain vigilant against incidents of identity theft and fraud. We have established a call center to answer your questions: (855) 935-6070.

**What Happened?** On January 29, 2021, Accellion informed Trinity Health of a security issue with its secure file transfer platform, used for sending secure email. Upon receiving this notice, Trinity Health immediately took the appliance offline and launched an investigation into the issue and its impact on both Trinity Health and our patients and colleagues. This investigation determined that certain files present on the appliance on January 20 were downloaded by an unknown user. The unauthorized user was able to take advantage of a previously unknown and unreported flaw in the security of the Accellion appliance.

**What Information is Involved?** Although the investigation is ongoing, on February 4, 2021, we determined file(s) were present on the appliance at the time of this event. The files contained certain protected health information, including some combination of the following, **patient's name, address, email, date of birth, healthcare provider, dates and types of health care services, medical record number, immunization type, lab results, medications, payment, payer name, and claims information.** <<b2b\_text\_1 (variable text sentence- SSN#, credit card information)>>

**What We Are Doing.** We take these matters extremely seriously. When we were alerted of the security issue, we immediately took steps to terminate access and use of the appliance and worked with Accellion to investigate the event. We also confirmed the security of our network. Additionally, while we go to great lengths to protect patient and colleague information entrusted to us, as part of our ongoing commitment to the security of information in our care, we are further evaluating our data security policies and procedures.

**What You Can Do.** We are providing notice of this event to you, so that you may take further steps to protect the patient's protected health information should you feel it is appropriate to do so. We encourage you to review the information in the attached "*Steps You Can Take to Protect Information.*"

Trinity Health is also offering the patient complimentary access to credit monitoring services as appropriate to the information impacted. Information on these services and enrollment directions are in the attached information.

**For More Information.** I want to assure you that we take the responsibility to safeguard protected health information very seriously. We apologize for any inconvenience or concern this situation may have caused you. If you have any additional questions or concerns, please do not hesitate to call (855) 935-6070 from 8:00 a.m. - 5:30 p.m. Central Time, Monday - Friday, or email [THresponse@kroll.com](mailto:THresponse@kroll.com)

Español (Spanish) <https://www.trinity-health.org/accellion-data-event/>

Sincerely,

Trinity Health

*Monica Lareau*

Trinity Health, Privacy Official

## Steps You Can Take to Protect Information

### Credit Monitoring Services:

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

You have until **July 4, 2021** to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

If you are under 18 and wish to activate identity monitoring services, please email us at [THresponse@kroll.com](mailto:THresponse@kroll.com) so that we can adjust the services offered as credit monitoring is not available to individuals under 18 years old.

### Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
888-298-0045	1-888-397-3742	833-395-6938

Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

**Additional Information**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.gov).

*For New York residents*, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.



## **TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You have been provided with access to the following services from Kroll:

### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



## About Trinity Health

Trinity Health, based in Livonia, Mich., is one of the largest multi-institutional Catholic health care systems in the nation, serving diverse communities that include more than 30 million people across 22 states. Trinity Health includes 92 hospitals, as well as 113 continuing care locations that include PACE programs, senior living facilities, and home care and hospice services. Its continuing care programs provide nearly 2.5 million visits annually. For more information, visit [www.trinity-health.org](http://www.trinity-health.org) and [Location Results \(trinity-health.org\)](http://www.trinity-health.org/location-results). Trinity Health provides information technology services for the health care system and some former members of the health system, including email hosting and file transfer services. Trinity Health functions as a business associate (as defined by HIPAA) to its member hospitals and affiliated medical groups.

### Trinity Health Current and Affected Former Member Organizations

Listed below are the locations of Trinity Health hospitals and medical groups affiliated with the hospitals

#### California (Fresno)

Saint Agnes Medical Center  
[www.samc.com](http://www.samc.com)

#### Connecticut (Hartford)

Trinity Health Of New England  
[www.trinityhealthofne.org](http://www.trinityhealthofne.org)

#### Delaware (Wilmington)

Trinity Health Mid-Atlantic  
[www.trinityhealthma.org](http://www.trinityhealthma.org)

#### Florida (Fort Lauderdale)

Holy Cross Health Fort Lauderdale  
[www.holy-cross.com](http://www.holy-cross.com)

#### Idaho (Boise, Nampa)

Saint Alphonsus Health System  
[www.saintalphonsus.org](http://www.saintalphonsus.org)

#### Illinois (Greater Chicago)

Loyola Medicine  
[www.loyolamedicine.org](http://www.loyolamedicine.org)

#### Mercy Hospital and Med. Center

[www.mercy-chicago.org](http://www.mercy-chicago.org)

#### Indiana (South Bend)

Saint Joseph Health System  
[www.sjmed.com](http://www.sjmed.com)

#### Iowa (Clinton, Sioux City, Dubuque, Mason City)

MercyOne  
[www.mercyone.org](http://www.mercyone.org)

#### Maryland (Silver Spring)

Holy Cross Health Silver Spring  
[www.holycrosshealth.org](http://www.holycrosshealth.org)

#### Massachusetts (Springfield)

Trinity Health Of New England  
[www.trinityhealthofne.org](http://www.trinityhealthofne.org)

#### Michigan (Southeast)

Saint Joseph Mercy Health System  
[www.stjoeshealth.org](http://www.stjoeshealth.org)

#### Mercy Health (West)

[www.mercyhealth.com](http://www.mercyhealth.com)

#### New York

St. Peters Health Partners (Albany)  
[www.sphp.com](http://www.sphp.com)

#### St. Joseph's Health (Syracuse)

[www.sjhsyr.org](http://www.sjhsyr.org)

#### New Jersey

St. Francis Medical Center (Trenton)  
[www.stfrancismedical.org](http://www.stfrancismedical.org)

#### Ohio (Columbus)

Mount Carmel Health System  
[www.mountcarmelhealth.com](http://www.mountcarmelhealth.com)

#### Oregon (Baker City, Ontario)

Saint Alphonsus Health System  
[www.saintalphonsus.org](http://www.saintalphonsus.org)

#### Pennsylvania (Greater Philadelphia)

Trinity Health Mid-Atlantic  
[www.trinityhealthma.org](http://www.trinityhealthma.org)

*On July 1, 2019 the below former Trinity Health locations joined Virtua Health. Trinity Health continued to provide information system services to these facilities in 2019 and 2020.*

#### [www.virtua.org](http://www.virtua.org)

Virtua Our Lady of Lourdes Hospital, formerly known as Our Lady of Lourdes Medical Center (Camden)

Virtua Willingboro Hospital, formerly known as Lourdes Medical Center of Burlington County (Burlington)

# Exhibit B





## Press Release

### ACCELLION RESPONDS TO RECENT FTA SECURITY INCIDENT

#### *Patch Released in 72 Hours with Minimal Impact*

Palo Alto, CA | January 12, 2021

Accellion, Inc., provider of the industry's first enterprise content firewall, today issued a statement about a recently reported security incident regarding one of its legacy products.

In mid-December, Accellion was made aware of a P0 vulnerability in its legacy File Transfer Appliance (FTA) software. Accellion FTA is a 20 year old product that specializes in large file transfers.

Accellion resolved the vulnerability and released a patch within 72 hours to the less than 50 customers affected.

Accellion's flagship enterprise content firewall platform, kiteworks, was not involved in any way. The kiteworks product has never reported an external P0 vulnerability during its four years in the marketplace. The Accellion enterprise content firewall deploys the most advanced security available and sets the standard for secure file sharing in the industry. Accellion is SOC2 certified and kiteworks is available in highly secure on-premise and hosted FedRAMP deployments. It provides organizations in highly regulated industries with complete visibility, security and control over the communication of IP, PII, PHI, and other sensitive content across email, file sharing, mobile, enterprise apps, web portals, SFTP, and automated inter-business workflows.

This website uses cookies to enhance your experience. By continuing to visit this site you agree to the use of cookies. To find out more about the cookies we use, see our Privacy Policy





please visit [Enterprise Content Firewall](#).

## About Accellion

The Accellion enterprise content firewall prevents data breaches and compliance violations from sensitive third party communications. With Accellion, CIOs and CISOs gain complete visibility, compliance and control over IP, PII, PHI, and other sensitive content across all third-party communication channels, providing [secure email](#), [secure file sharing](#), secure mobile file sharing, enterprise app and Microsoft Office plugins, secure web forms, secure file transfer like SFTP, and enterprise workflow automation. Accellion has protected more than 25 million end users at more than 3,000 global corporations and government agencies, including NYC Health + Hospitals; KPMG; Kaiser Permanente; National Park Service; Tyler Technologies; and the National Institute for Standards and Technology (NIST). For more information please visit [www.accellion.com](http://www.accellion.com) or call (650) 485-4300. Follow Accellion on: [LinkedIn](#), [Twitter](#), and [Accellion's Blog](#).

### Media Contacts

Rob Dougherty

(650) 687-3163

[robert.dougherty@accellion.com](mailto:robert.dougherty@accellion.com)

*Accellion and kiteworks are registered trademarks of Accellion, Inc. in the US and other countries. All other trademarks contained herein are the property of their respective owners.*

## SIGN UP FOR THE LATEST BLOG POSTS AND NEWS

First Name\*

This website uses cookies to enhance your experience. By continuing to visit this site you agree to the use of cookies. To find out more about the cookies we use, see our [Privacy Policy](#)





Find it faster with search

**SUBMIT**

## CONTACT US

### Sales

+1-650-637-3130

[sales@accellion.com](mailto:sales@accellion.com)

### Stay Connected

### Support

+1-888-654-3778

[support@accellion.com](mailto:support@accellion.com)

## PLATFORM

Platform Overview

Communication Consolidation

Unified Visibility

Unified Security

Unified Compliance

## INDUSTRY

Government

Healthcare

Financial Services

Legal

Manufacturing and Engineering

Higher Education

## CAPABILITIES

CISO Dashboard

Secure File Sharing

Secure Email

Secure Mobile

Remote Work Security

## COMPLIANCE

HIPAA

GDPR

FedRAMP

FIPS

SOC 2

This website uses cookies to enhance your experience. By continuing to visit this site you agree to the use of cookies. To find out more about the cookies we use, see our Privacy Policy



[Boardroom](#)[Communications](#)[Secure Managed File](#)[Transfer](#)[SFTP Server](#)[Secure Content Access](#)[Microsoft Office 365](#)[Plugins](#)

## RESOURCES

[Resource Center](#)[Case Studies](#)[Customers](#)[eBooks](#)[Product Briefs](#)[Webinars](#)[Whitepapers](#)[Developer](#)[Blog](#)

## COMPANY

[About Us](#)[Contact Us](#)[Management Team](#)[Investors](#)[Partners](#)[Press & Media](#)[Events](#)[Careers](#)[Pricing](#)

© 2021 ACCELLION. All rights reserved.

[Privacy Policy](#) | [Legal](#)

This website uses cookies to enhance your experience. By continuing to visit this site you agree to the use of cookies. To find out more about the cookies we use, see our [Privacy Policy](#)



# Exhibit C



## Press Release

### ACCELLION PROVIDES UPDATE TO RECENT FTA SECURITY INCIDENT

#### *All Known Vulnerabilities Closed and Migration Efforts Continue*

Palo Alto, CA | February 1, 2021

Accellion, Inc., provider of the industry's first enterprise content firewall, today issued an update on the recently reported security incident regarding FTA, Accellion's legacy large file transfer product.

Accellion FTA, a 20 year old product nearing end-of life, was the target of a sophisticated cyberattack. All FTA customers were promptly notified of the attack on December 23, 2020. At this time, Accellion has patched all known FTA vulnerabilities exploited by the attackers and has added new monitoring and alerting capabilities to flag anomalies associated with these attack vectors.

## Accellion kiteworks Content Firewall Unaffected

All vulnerabilities are limited exclusively to FTA. They do not in any way impact Accellion's enterprise content firewall platform known as kiteworks. The vast majority of Accellion's clients reside on the kiteworks platform, which is built on an entirely different code base, using state-of-the-art security architecture, and a segregated, secure development process.

In mid-December, Accellion was made aware of a zero-day vulnerability in its legacy FTA software. Accellion released a fix within 72 hours. This initial incident was the beginning of a concerted cyberattack on the Accellion FTA product that continued into January 2021.



## Accellion FTA Customers Encouraged to Upgrade to kiteworks

“Our latest release of FTA has addressed all known vulnerabilities at this time,” commented Frank Balonis, Accellion’s Chief Information Security Officer. “Future exploits, however, are a constant threat. We have encouraged all FTA customers to migrate to kiteworks for the last three years and have accelerated our FTA end-of-life plans in light of these attacks. We remain committed to assisting our FTA customers, but strongly urge them to migrate to kiteworks as soon as possible.”

FTA’s maturity notwithstanding, these exploits demonstrate a highly sophisticated attack. In 2021, every software security provider must not only demonstrate secure software architecture but must also be proficient at cyberwarfare. Accellion is uniformly committed to protecting its customers and their supply chain partners from cyber criminals by preventing breaches and compliance violations, rapidly responding to cyberattacks in process, and mitigating the impact of incursions with extensive forensics and customer support. In regard to this incident, Accellion is contracting with an industry-leading cybersecurity forensics firm to conduct a compromise assessment and will share their findings when available.

FTA customers are encouraged to contact Accellion customer support for additional information at [support@accellion.com](mailto:support@accellion.com).

To learn more how the flagship Accellion kiteworks platform helps organizations secure their third party communications, please visit [Enterprise Content Firewall](#).

## About Accellion





third-party communication channels, providing secure email, secure file sharing, secure mobile file sharing, enterprise app and Microsoft Office plugins, secure web forms, secure file transfer like SFTP, and enterprise workflow automation. Accellion has protected more than 25 million end users at more than 3,000 global corporations and government agencies, including NYC Health + Hospitals; KPMG; Kaiser Permanente; National Park Service; Tyler Technologies; and the National Institute for Standards and Technology (NIST). For more information please visit [www.accellion.com](http://www.accellion.com) or call (650) 485-4300. Follow Accellion on: [LinkedIn](#), [Twitter](#), and [Accellion's Blog](#).

### Media Contacts

Rob Dougherty

(650) 687-3163

[robert.dougherty@accellion.com](mailto:robert.dougherty@accellion.com)

*Accellion and kiteworks are registered trademarks of Accellion, Inc. in the US and other countries. All other trademarks contained herein are the property of their respective owners.*

## SIGN UP FOR THE LATEST BLOG POSTS AND NEWS

First Name\*

Last Name\*

Company\*

Business Email\*

**SUBMIT**



## Sales

+1-650-687-3130

[sales@accellion.com](mailto:sales@accellion.com)

## Support

+1-888-654-3778

[support@accellion.com](mailto:support@accellion.com)

## Stay Connected

### PLATFORM

Platform Overview

Communication Consolidation

Unified Visibility

Unified Security

Unified Compliance

### INDUSTRY

Government

Healthcare

Financial Services

Legal

Manufacturing and Engineering

Higher Education

### CAPABILITIES

CISO Dashboard

Secure File Sharing

Secure Email

Secure Mobile

Remote Work Security

Enterprise App

Sharing

Secure Web Forms

Secure Collaboration

Virtual Data Rooms

Boardroom

Communications

Secure Managed File

Transfer

### COMPLIANCE

HIPAA

GDPR

FedRAMP

FIPS

SOC 2

CMMC

Data Sovereignty

eDiscovery

SETD Series



---

Plugins

## RESOURCES

[Resource Center](#)

[Case Studies](#)

[Customers](#)

[eBooks](#)

[Product Briefs](#)

[Webinars](#)

[Whitepapers](#)

[Developer](#)

[Blog](#)

## COMPANY

[About Us](#)

[Contact Us](#)

[Management Team](#)

[Investors](#)

[Partners](#)

[Press & Media](#)

[Events](#)

[Careers](#)

[Pricing](#)

© 2021 ACCELLION. All rights reserved.

[Privacy Policy](#) | [Legal](#)

# EXHIBIT B

SUM-100

# SUMMONS (CITACION JUDICIAL)

## NOTICE TO DEFENDANT: (AVISO AL DEMANDADO):

TRINITY HEALTH CORPORATION; and DOE DEFENDANTS 1-100

## YOU ARE BEING SUED BY PLAINTIFF: (LO ESTÁ DEMANDANDO EL DEMANDANTE):

JANE DOE, individually and on behalf of all others similarly situated

FOR COURT USE ONLY  
(SOLO PARA USO DE LA CORTE)

E-FILED

5/21/2021

Superior Court of California  
County of Fresno

By: A. Rodriguez, Deputy

NOTICE! You have been sued. The court may decide against you without your being heard unless you respond within 30 days. Read the information below.

You have 30 CALENDAR DAYS after this summons and legal papers are served on you to file a written response at this court and have a copy served on the plaintiff. A letter or phone call will not protect you. Your written response must be in proper legal form if you want the court to hear your case. There may be a court form that you can use for your response. You can find these court forms and more information at the California Courts Online Self-Help Center ([www.courtinfo.ca.gov/selfhelp](http://www.courtinfo.ca.gov/selfhelp)), your county law library, or the courthouse nearest you. If you cannot pay the filing fee, ask the court clerk for a fee waiver form. If you do not file your response on time, you may lose the case by default, and your wages, money, and property may be taken without further warning from the court.

There are other legal requirements. You may want to call an attorney right away. If you do not know an attorney, you may want to call an attorney referral service. If you cannot afford an attorney, you may be eligible for free legal services from a nonprofit legal services program. You can locate these nonprofit groups at the California Legal Services Web site ([www.lawhelpcalifornia.org](http://www.lawhelpcalifornia.org)), the California Courts Online Self-Help Center ([www.courtinfo.ca.gov/selfhelp](http://www.courtinfo.ca.gov/selfhelp)), or by contacting your local court or county bar association. NOTE: The court has a statutory lien for waived fees and costs on any settlement or arbitration award of \$10,000 or more in a civil case. The court's lien must be paid before the court will dismiss the case. ¡AVISO! Lo han demandado. Si no responde dentro de 30 días, la corte puede decidir en su contra sin escuchar su versión. Lea la información a continuación.

Tiene 30 DÍAS DE CALENDARIO después de que le entreguen esta citación y papeles legales para presentar una respuesta por escrito en esta corte y hacer que se entregue una copia al demandante. Una carta o una llamada telefónica no lo protegen. Su respuesta por escrito tiene que estar en formato legal correcto si desea que procesen su caso en la corte. Es posible que haya un formulario que usted pueda usar para su respuesta. Puede encontrar estos formularios de la corte y más información en el Centro de Ayuda de las Cortes de California ([www.sucorte.ca.gov](http://www.sucorte.ca.gov)), en la biblioteca de leyes de su condado o en la corte que le quede más cerca. Si no puede pagar la cuota de presentación, pida al secretario de la corte que le dé un formulario de exención de pago de cuotas. Si no presenta su respuesta a tiempo, puede perder el caso por incumplimiento y la corte le podrá quitar su sueldo, dinero y bienes sin más advertencia.

Hay otros requisitos legales. Es recomendable que llame a un abogado inmediatamente. Si no conoce a un abogado, puede llamar a un servicio de remisión a abogados. Si no puede pagar a un abogado, es posible que cumpla con los requisitos para obtener servicios legales gratuitos de un programa de servicios legales sin fines de lucro. Puede encontrar estos grupos sin fines de lucro en el sitio web de California Legal Services, ([www.lawhelpcalifornia.org](http://www.lawhelpcalifornia.org)), en el Centro de Ayuda de las Cortes de California, ([www.sucorte.ca.gov](http://www.sucorte.ca.gov)) o poniéndose en contacto con la corte o el colegio de abogados locales. AVISO: Por ley, la corte tiene derecho a reclamar las cuotas y los costos exentos por imponer un gravamen sobre cualquier recuperación de \$10,000 ó más de valor recibida mediante un acuerdo o una concesión de arbitraje en un caso de derecho civil. Tiene que pagar el gravamen de la corte antes de que la corte pueda desechar el caso.

The name and address of the court is:

(El nombre y dirección de la corte es): FRESNO COUNTY SUPERIOR COURT  
1130 O Street  
Fresno, CA 93724-0002

CASE NUMBER: (Número del Caso):

21CECG01454

The name, address, and telephone number of plaintiff's attorney, or plaintiff without an attorney, is: (El nombre, la dirección y el número de teléfono del abogado del demandante, o del demandante que no tiene abogado, es):

Patrick N. Keegan, Esq., KEEGAN &amp; BAKER, LLP, 2292 Faraday Avenue, Suite 100, Carlsbad, CA 92008; (760) 929-9303

DATE:

(Fecha) 5/21/2021

Clerk, by

(Secretario) A. Rodriguez

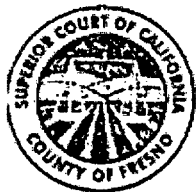
Deputy

(Adjunto)

(For proof of service of this summons, use Proof of Service of Summons (form POS-010).)

(Para prueba de entrega de esta citación use el formulario Proof of Service of Summons, (POS-010).)

(SEAL)



### NOTICE TO THE PERSON SERVED: You are served

1. ☐ as an individual defendant.
2. ☐ as the person sued under the fictitious name of (specify):
3. ☒ on behalf of (specify): Trinity Health Corporation  
under: ☒ CCP 416.10 (corporation) ☐ CCP 416.60 (minor)  
☐ CCP 416.20 (defunct corporation) ☐ CCP 416.70 (conservatee)  
☐ CCP 416.40 (association or partnership) ☐ CCP 416.90 (authorized person)  
☐ other (specify):
4. ☐ by personal delivery on (date)

Page 1 of 1

# EXHIBIT C

ATTORNEY OR PARTY WITHOUT ATTORNEY (Name, State Bar number, and address): Patrick N. Keegan, Esq. (SBN 167698) KEEGAN & BAKER, LLP 2292 Faraday Avenue, Suite 100, Carlsbad, CA 92008		FOR COURT USE ONLY  <b>E-FILED</b> 5/20/2021 7:23 PM Superior Court of California County of Fresno By: A. Rodriguez, Deputy
TELEPHONE NO.: (760) 929-9303      FAX NO. (Optional): (760) 929-9260 ATTORNEY FOR (Name): Plaintiff		
<b>SUPERIOR COURT OF CALIFORNIA, COUNTY OF FRESNO</b> STREET ADDRESS: 1130 O Street MAILING ADDRESS: 1130 O Street CITY AND ZIP CODE: Fresno, CA 93724-0002 BRANCH NAME:		
CASE NAME: JANE DOE v. TRINITY HEALTH CORPORATION		
<b>CIVIL CASE COVER SHEET</b> <input checked="" type="checkbox"/> <b>Unlimited</b> (Amount demanded exceeds \$25,000) <input type="checkbox"/> <b>Limited</b> (Amount demanded is \$25,000)		CASE NUMBER: <b>21CECG01454</b>  JUDGE: DEPT.:
<b>Complex Case Designation</b> <input type="checkbox"/> Counter <input type="checkbox"/> Joinder Filed with first appearance by defendant (Cal. Rules of Court, rule 3.402)		

*Items 1–6 below must be completed (see instructions on page 2).*

1. Check **one** box below for the case type that best describes this case:

<b>Auto Tort</b> <input type="checkbox"/> Auto (22) - <input type="checkbox"/> Uninsured motorist (46) <b>Other PI/PD/WD (Personal Injury/Property Damage/Wrongful Death) Tort</b> <input type="checkbox"/> Asbestos (04) <input type="checkbox"/> Product liability (24) <input type="checkbox"/> Medical malpractice (45) <input type="checkbox"/> Other PI/PD/WD (23) <b>Non-PI/PD/WD (Other) Tort</b> <input checked="" type="checkbox"/> Business tort/unfair business practice (07) <input type="checkbox"/> Civil rights (08) <input type="checkbox"/> Defamation (13) <input type="checkbox"/> Fraud (16) <input type="checkbox"/> Intellectual property (19) <input type="checkbox"/> Professional negligence (25) <input type="checkbox"/> Other non-PI/PD/WD tort (35) <b>Employment</b> <input type="checkbox"/> Wrongful termination (36) <input type="checkbox"/> Other employment (15)	<b>Contract</b> <input type="checkbox"/> Breach of contract/warranty (06) <input type="checkbox"/> Rule 3.740 collections (09) <input type="checkbox"/> Other collections (09) <input type="checkbox"/> Insurance coverage (18) <input type="checkbox"/> Other contract (37) <b>Real Property</b> <input type="checkbox"/> Eminent domain/Inverse condemnation (14) <input type="checkbox"/> Wrongful eviction (33) <input type="checkbox"/> Other real property (26) <b>Unlawful Detainer</b> <input type="checkbox"/> Commercial (31) <input type="checkbox"/> Residential (32) <input type="checkbox"/> Drugs (38) <b>Judicial Review</b> <input type="checkbox"/> Asset forfeiture (05) <input type="checkbox"/> Petition re: arbitration award (11) <input type="checkbox"/> Writ of mandate (02) <input type="checkbox"/> Other judicial review (39)	<b>Provisionally Complex Civil Litigation (Cal. Rules of Court, rules 3.400–3.403)</b> <input type="checkbox"/> Antitrust/Trade regulation (03) <input type="checkbox"/> Construction defect (10) <input type="checkbox"/> Mass tort (40) <input type="checkbox"/> Securities litigation (28) <input type="checkbox"/> Environmental/Toxic tort (30) <input type="checkbox"/> Insurance coverage claims arising from the above listed provisionally complex case types (41) <b>Enforcement of Judgment</b> <input type="checkbox"/> Enforcement of judgment (20) <b>Miscellaneous Civil Complaint</b> <input type="checkbox"/> RICO (27) <input type="checkbox"/> Other complaint ( <i>not specified above</i> ) (42) <b>Miscellaneous Civil Petition</b> <input type="checkbox"/> Partnership and corporate governance (21) <input type="checkbox"/> Other petition ( <i>not specified above</i> ) (43)
---	--	--

2. This case ☐ is ☒ is not complex under rule 3.400 of the California Rules of Court. If the case is complex, mark the factors requiring exceptional judicial management:
- |  |  |
|--|--|
| a. <input type="checkbox"/> Large number of separately represented parties<br>b. <input type="checkbox"/> Extensive motion practice raising difficult or novel issues that will be time-consuming to resolve<br>c. <input type="checkbox"/> Substantial amount of documentary evidence | d. <input type="checkbox"/> Large number of witnesses<br>e. <input type="checkbox"/> Coordination with related actions pending in one or more courts in other counties, states, or countries, or in a federal court<br>f. <input type="checkbox"/> Substantial postjudgment judicial supervision |
|--|--|
3. Remedies sought (*check all that apply*): a. ☒ monetary    b. ☒ nonmonetary; declaratory or injunctive relief    c. ☐ punitive
4. Number of causes of action (*specify*): Three
5. This case ☒ is ☐ is not a class action suit.
6. If there are any known related cases, file and serve a notice of related case. (*You may use form CM-015.*)
- Date: May 20, 2021
- Patrick N. Keegan, Esq. \_\_\_\_\_

(TYPE OR PRINT NAME)

(SIGNATURE OF PARTY OR ATTORNEY FOR PARTY)

**NOTICE**

- Plaintiff must file this cover sheet with the first paper filed in the action or proceeding (except small claims cases or cases filed under the Probate Code, Family Code, or Welfare and Institutions Code). (Cal. Rules of Court, rule 3.220.) Failure to file may result in sanctions.
- File this cover sheet in addition to any cover sheet required by local court rule.
- If this case is complex under rule 3.400 et seq. of the California Rules of Court, you must serve a copy of this cover sheet on all other parties to the action or proceeding.
- Unless this is a collections case under rule 3.740 or a complex case, this cover sheet will be used for statistical purposes only.

Page 1 of 2



**INSTRUCTIONS ON HOW TO COMPLETE THE COVER SHEET**

**To Plaintiffs and Others Filing First Papers.** If you are filing a first paper (for example, a complaint) in a civil case, you **must** complete and file, along with your first paper, the Civil Case Cover Sheet contained on page 1. This information will be used to compile statistics about the types and numbers of cases filed. You must complete items 1 through 6 on the sheet. In item 1, you must check **one** box for the case type that best describes the case. If the case fits both a general and a more specific type of case listed in item 1, check the more specific one. If the case has multiple causes of action, check the box that best indicates the **primary** cause of action. To assist you in completing the sheet, examples of the cases that belong under each case type in item 1 are provided below. A cover sheet must be filed only with your initial paper. Failure to file a cover sheet with the first paper filed in a civil case may subject a party, its counsel, or both to sanctions under rules 2.30 and 3.220 of the California Rules of Court.

**To Parties in Rule 3.740 Collections Cases.** A "collections case" under rule 3.740 is defined as an action for recovery of money owed in a sum stated to be certain that is not more than \$25,000, exclusive of interest and attorney's fees, arising from a transaction in which property, services, or money was acquired on credit. A collections case does not include an action seeking the following: (1) tort damages, (2) punitive damages, (3) recovery of real property, (4) recovery of personal property, or (5) a prejudgment writ of attachment. The identification of a case as a rule 3.740 collections case on this form means that it will be exempt from the general time-for-service requirements and case management rules, unless a defendant files a responsive pleading. A rule 3.740 collections case will be subject to the requirements for service and obtaining a judgment in rule 3.740.

**To Parties in Complex Cases.** In complex cases only, parties must also use the Civil Case Cover Sheet to designate whether the case is complex. If a plaintiff believes the case is complex under rule 3.400 of the California Rules of Court, this must be indicated by completing the appropriate boxes in items 1 and 2. If a plaintiff designates a case as complex, the cover sheet must be served with the complaint on all parties to the action. A defendant may file and serve no later than the time of its first appearance a joinder in the plaintiff's designation, a counter-designation that the case is not complex, or, if the plaintiff has made no designation, a designation that the case is complex.

**CASE TYPES AND EXAMPLES****Auto Tort**

Auto (22)—Personal Injury/Property Damage/Wrongful Death  
Uninsured Motorist (46) (*if the case involves an uninsured motorist claim subject to arbitration, check this item instead of Auto*)

**Other PI/PD/WD (Personal Injury/Property Damage/Wrongful Death) Tort**

Asbestos (04)  
Asbestos Property Damage  
Asbestos Personal Injury/Wrongful Death  
Product Liability (*not asbestos or toxic/environmental*) (24)  
Medical Malpractice (45)  
Medical Malpractice—Physicians & Surgeons  
Other Professional Health Care Malpractice  
Other PI/PD/WD (23)  
Premises Liability (e.g., slip and fall)  
Intentional Bodily Injury/PD/WD (e.g., assault, vandalism)  
Intentional Infliction of Emotional Distress  
Negligent Infliction of Emotional Distress  
Other PI/PD/WD

**Non-PI/PD/WD (Other) Tort**

Business Tort/Unfair Business Practice (07)  
Civil Rights (e.g., discrimination, false arrest) (*not civil harassment*) (08)  
Defamation (e.g., slander, libel) (13)  
Fraud (16)  
Intellectual Property (19)  
Professional Negligence (25)  
Legal Malpractice  
Other Professional Malpractice (*not medical or legal*)  
Other Non-PI/PD/WD Tort (35)  
**Employment**  
Wrongful Termination (36)  
Other Employment (15)

**Contract**

Breach of Contract/Warranty (06)  
Breach of Rental/Lease  
Contract (*not unlawful detainer or wrongful eviction*)  
Contract/Warranty Breach—Seller Plaintiff (*not fraud or negligence*)  
Negligent Breach of Contract/Warranty  
Other Breach of Contract/Warranty  
Collections (e.g., money owed, open book accounts) (09)  
Collection Case—Seller Plaintiff  
Other Promissory Note/Collections Case  
Insurance Coverage (*not provisionally complex*) (18)  
Auto Subrogation  
Other Coverage  
Other Contract (37)  
Contractual Fraud  
Other Contract Dispute

**Real Property**

Eminent Domain/Inverse Condemnation (14)  
Wrongful Eviction (33)  
Other Real Property (e.g., quiet title) (26)  
Writ of Possession of Real Property  
Mortgage Foreclosure  
Quiet Title  
Other Real Property (*not eminent domain, landlord/tenant, or foreclosure*)

**Unlawful Detainer**

Commercial (31)  
Residential (32)  
Drugs (38) (*if the case involves illegal drugs, check this item; otherwise, report as Commercial or Residential*)

**Judicial Review**

Asset Forfeiture (05)  
Petition Re: Arbitration Award (11)  
Writ of Mandate (02)  
Writ—Administrative Mandamus  
Writ—Mandamus on Limited Court Case Matter  
Writ—Other Limited Court Case Review  
Other Judicial Review (39)  
Review of Health Officer Order  
Notice of Appeal—Labor Commissioner Appeals

**Provisionally Complex Civil Litigation (Cal. Rules of Court Rules 3.400–3.403)**

Antitrust/Trade Regulation (03)  
Construction Defect (10)  
Claims Involving Mass Tort (40)  
Securities Litigation (28)  
Environmental/Toxic Tort (30)  
Insurance Coverage Claims (*arising from provisionally complex case type listed above*) (41)

**Enforcement of Judgment**

Enforcement of Judgment (20)  
Abstract of Judgment (Out of County)  
Confession of Judgment (*non-domestic relations*)  
Sister State Judgment  
Administrative Agency Award (*not unpaid taxes*)  
Petition/Certification of Entry of Judgment on Unpaid Taxes  
Other Enforcement of Judgment Case

**Miscellaneous Civil Complaint**

RICO (27)  
Other Complaint (*not specified above*) (42)  
Declaratory Relief Only  
Injunctive Relief Only (*non-harassment*)  
Mechanics Lien  
Other Commercial Complaint Case (*non-tort/non-complex*)  
Other Civil Complaint (*non-tort/non-complex*)

**Miscellaneous Civil Petition**

Partnership and Corporate Governance (21)  
Other Petition (*not specified above*) (43)  
Civil Harassment  
Workplace Violence  
Elder/Dependent Adult Abuse  
Election Contest  
Petition for Name Change  
Petition for Relief From Late Claim  
Other Civil Petition

# EXHIBIT D

<b>SUPERIOR COURT OF CALIFORNIA • COUNTY OF FRESNO</b> <b>Civil Unlimited Department, Central Division</b> 1130 "O" Street Fresno, California 93724-0002 <b>(559) 457-1900</b>	FOR COURT USE ONLY  5/21/2021  Filed by Court
TITLE OF CASE:  <b>Jane Doe vs. Trinity Health Corporation</b>	
<b>NOTICE OF CASE MANAGEMENT CONFERENCE AND ASSIGNMENT OF JUDGE FOR ALL PURPOSES</b>	CASE NUMBER: <b>21CECG01454</b>

**To All Parties and their Attorneys of Record: Patrick N Keegan**

This case has been assigned to **Rosemary McGuire**, Judge for **all purposes**.  
 All future hearings will be scheduled before this assigned judge.

You are required to appear at a Case Management Conference on **09/15/2021** at **3:30 PM** in **Department 402** of the court located at 1130 "O" Street, **Fresno, California**.

You must comply with the requirements set forth in Fresno Superior Court Local Rule Chapter 2.

Failure to appear at the conference may result in imposition of sanctions, waiver of jury trial, or other adverse consequences.

**Defendants:** Appearance at the Case Management Conference does not excuse you from having to file your response in proper legal form within 30 days after the Summons is served on you. You could lose the case if you do not file your response on time. If you do not know an attorney, and do not have one, you may call an attorney referral service or a legal aid office (*listed in the phone book*).

#### DECLARATION

I declare under penalty of perjury under the laws of the State of California that I gave a copy of the **Notice of Case Management and Assignment of Judge for All Purposes** to the person who presented this case for filing.

Date: 5/21/2021 Clerk, by Ashley Rodriguez  , Deputy

# EXHIBIT E

## State of Indiana Office of the Secretary of State

### Certified Copies

To Whom These Presents Come, Greeting:

I, HOLLI SULLIVAN, Secretary of State of Indiana, do hereby certify that I am, by virtue of the laws of the State of Indiana, the custodian of the corporate records and the proper official to execute this certificate.

I further certify that this is a true and complete copy of this 4 page document consisting of the following records filed in this office:

Certification Date: June 15, 2021  
Business Name: TRINITY HEALTH CORPORATION  
Business ID: 197811-279

Transaction	Date Filed	No. of pages
Business Entity Report	11/24/2020	4
Total No. of pages		4



In Witness Whereof, I have caused to be affixed my signature and the seal of the State of Indiana, at the City of Indianapolis, June 15, 2021

HOLLI SULLIVAN  
SECRETARY OF STATE

197811-279 / 13816728

All certificates should be validated here: <https://bsd.sos.in.gov/ValidateCertificate>

Expires on July 15, 2021.

**APPROVED AND FILED**  
CONNIE LAWSON  
INDIANA SECRETARY OF STATE  
11/24/2020 11:59 AM

**BUSINESS ENTITY REPORT****NAME AND PRINCIPAL OFFICE ADDRESS**

<b>BUSINESS ID</b>	197811-279
<b>BUSINESS TYPE</b>	Domestic Nonprofit Corporation
<b>BUSINESS NAME</b>	TRINITY HEALTH CORPORATION
<b>ENTITY CREATION DATE</b>	11/10/1978
<b>JURISDICTION OF FORMATION</b>	Indiana
<b>PRINCIPAL OFFICE ADDRESS</b>	20555 VICTOR PARKWAY, LIVONIA, MI, 48152, USA

**YEARS FILED**

<b>YEARS</b>	2020/2021
--------------	-----------

**EFFECTIVE DATE**

<b>EFFECTIVE DATE</b>	11/24/2020
<b>EFFECTIVE TIME</b>	11:59 AM

**REGISTERED OFFICE AND ADDRESS**

<b>REGISTERED AGENT TYPE</b>	Business Commercial Registered Agent
<b>NAME</b>	C T CORPORATION SYSTEM
<b>ADDRESS</b>	334 North Senate Avenue, Indianapolis, IN, 46204, USA

**APPROVED AND FILED**  
**CONNIE LAWSON**  
**INDIANA SECRETARY OF STATE**  
11/24/2020 11:59 AM

**PRINCIPAL(S)**

**TITLE** Director  
**NAME** George Philip  
**ADDRESS** 208 Kelly Circle, Altamont, NY, 12009, USA

**TITLE** Director  
**NAME** Larry Warren  
**ADDRESS** 1970 Balmoral Drive, Detroit, MI, 48203, USA

**TITLE** Director  
**NAME** David Southwell  
**ADDRESS** 700 Scotts Bay Drive, Indian River, MI, 49749, USA

**TITLE** Director  
**NAME** Roberta Waite, EdD, APRN, CNS-BC, FAAN  
**ADDRESS** 1505 Race Street, Bellet Bldg. 527, MS 1030, Philadelphia, PA, 19102, USA

**TITLE** Director  
**NAME** Joseph Betancourt, MD  
**ADDRESS** Massachusetts General Hospital, 50 Staniford, 9th floor, Suite 901, Boston, MA, 02114, USA

**TITLE** Director  
**NAME** James D. Bentley, PhD  
**ADDRESS** 13106 Jingle Lane, Silver Spring, MD, 20906, USA

**TITLE** Director  
**NAME** Mary Catherine Karl, CPA  
**ADDRESS** 4951 W. Bay Way Drive, Tampa, FL, 33629, USA

**TITLE** President  
**NAME** Michael Slubowski  
**ADDRESS** 20555 Victor Parkway, Livonia, MI, 48152, USA

**TITLE** Director  
**NAME** Mary M Fanning, RSM  
**ADDRESS** 20555 Victor Parkway, Livonia, MI, 48152, USA



**APPROVED AND FILED**  
**CONNIE LAWSON**  
**INDIANA SECRETARY OF STATE**  
11/24/2020 11:59 AM

**TITLE** Treasurer  
**NAME** Cynthia Clemence  
**ADDRESS** 20555 Victor Parkway, Livonia, MI, 48152, USA

**TITLE** Secretary  
**NAME** Linda Ross, Esq  
**ADDRESS** 20555 Victor Parkway, Livonia, MI, 48152, USA

**TITLE** Director  
**NAME** Joan Marie Steadman, CSC  
**ADDRESS** 20555 Victor Parkway, Livonia, MI, 48152, USA

**TITLE** Director  
**NAME** Kevin Barnett  
**ADDRESS** 20555 Victor Parkway, Livonia, MI, 48152, USA

**TITLE** Director  
**NAME** Larry Warren  
**ADDRESS** 20555 Victor Parkway, Livonia, MI, 48152, USA

**TITLE** Director  
**NAME** Rita Brogley  
**ADDRESS** 20555 Victor Parkway, Livonia, MI, 48152, USA

**TITLE** Director  
**NAME** Linda Falquette RSM  
**ADDRESS** 20555 Victor Parkway, Livonia, MI, 48152, USA

**TITLE** Director  
**NAME** Barrett Hatches  
**ADDRESS** 20555 Victor Parkway, Livonia, MI, 48152, USA

**TITLE** Asst. Secretary  
**NAME** Joshua Moore  
**ADDRESS** 20555 Victor Parkway, Livonia, MI, 48152, USA

**APPROVED AND FILED**  
CONNIE LAWSON  
INDIANA SECRETARY OF STATE  
11/24/2020 11:59 AM

**SIGNATURE**

IN WITNESS WHEREOF, THE UNDERSIGNED HEREBY VERIFIES, SUBJECT TO THE PENALTIES OF PERJURY, THAT THE STATEMENTS CONTAINED HEREIN ARE TRUE, THIS DAY **November 24, 2020**.

**SIGNATURE**

Kary Smolarek

**TITLE**

Authorized Agent

Business ID : 197811-279

Filing No. : 8797071